PRIMERGY

B7FY-2091-01

# LAN 拡張ボード（1Gbps）取扱説明書

# 1Gbit/s Ethernet I/O Module User's Guide

（PG-LND201）

J

E

FUJITSU

# はじめに

このたびは、弊社の LAN 拡張ボード（1Gbps）（PG-LND201）をお買い上げいただき、誠にありがとうございます。
本製品は、弊社のサーバブレードの拡張ボードスロットに搭載し、LAN（Local Area Network）システムの構築に使用できます。
本書は、LAN 拡張ボード、LAN ドライバ（Windows 用）について説明します。ご使用になる前に、本書をよくお読みになり、正しい取り扱いをされますようお願いいたします。
LAN ドライバの詳細については、サーバブレードに添付されたマニュアル、または弊社のインターネット情報ページ（http://primeserver.fujitsu.com/primergy/）を参照してください。

2007 年 5 月

**安全にお使いいただくために**

本書には、本製品を安全に正しくお使いいただくための重要な情報が記載されています。
本製品をお使いになる前に、本書を熟読してください。特に、本書の「安全上のご注意」をよくお読みになり、理解されたうえで本製品をお使いください。
また本書は、本製品の使用中にいつでもご覧になれるよう大切に保管してください。

**注 意**

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づく第二種情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

**本製品のハイセイフティ用途での使用について**

本製品は、一般事務用、パーソナル用、家庭用、通常の産業用等の一般的用途を想定して設計・製造されているものであり、原子力施設における核反応制御、航空機自動飛行制御、航空交通管制、大量輸送システムにおける運行制御、生命維持のための医療器具、兵器システムにおけるミサイル発射制御など、極めて高度な安全性が要求され、仮に当該安全性が確保されない場合、直接生命・身体に対する重大な危険性を伴う用途（以下「ハイセイフティ用途」という）に使用されるよう設計・製造されたものではございません。お客様は、当該ハイセイフティ用途に要する安全性を確保する措置を施すことなく、本製品を使用しないでください。ハイセイフティ用途に使用される場合は、弊社の担当営業までご相談ください。

当社のドキュメントには「外国為替および外国貿易管理法」に基づく特定技術が含まれていることがあります。特定技術が含まれている場合は、当該ドキュメントを輸出または非居住者に提供するとき、同法に基づく許可が必要となります。

# 本書の表記

## ■警告表示

本書ではいろいろな絵表示を使っています。これは本製品を安全に正しくお使いいただき、あなたや他の人々に加えられるおそれのある危害や損害を未然に防止するための目印となるものです。その表示と意味は次のようになっています。内容をよくご理解の上、お読みください。

| | |
|---|---|
| ⚠警告 | この表示を無視して、誤った取り扱いをすると、人が死亡する可能性または重傷を負う可能性があることを示しています。 |
| ⚠注意 | この表示を無視して、誤った取り扱いをすると、人が損害を負う可能性があること、および物的損害のみが発生する可能性があることを示しています。 |

また、危害や損害の内容がどのようなものかを示すために、上記の絵表示と同時に次の記号を使用しています。

| | |
|---|---|
| | △で示した記号は、警告・注意を促す内容であることを告げるものです。記号の中やその脇には、具体的な警告内容が示されています。 |
| | ⃠で示した記号は、してはいけない行為（禁止行為）であることを告げるものです。記号の中やその脇には、具体的な禁止内容が示されています。 |
| | ●で示した記号は、必ず従っていただく内容であることを告げるものです。記号の中やその脇には、具体的な指示内容が示されています。 |

## ■本文中の記号

本文中に記載されている記号には、次のような意味があります。

| 記号 | 意味 |
|---|---|
| | お使いになる際の注意点や、してはいけないことを記述しています。必ずお読みください。 |
| | ハードウェアやソフトウェアを正しく動作させるために必要なことが書いてあります。必ずお読みください。 |
| → | 参照ページや参照マニュアルを示しています。 |

## ■コマンド入力（キー入力）

CD-ROM ドライブのドライブ名を、[CD-ROM ドライブ] で表記しています。入力の際は、お使いの環境に合わせて、ドライブ名を入力してください。

[CD-ROMドライブ]:¥Setup.exe

J

## ■製品の呼び方

本文中の製品名称を次のように略して表記します。

| 製品名称 | 本文中の表記 | |
|---|---|---|
| LAN 拡張ボード（1Gbps）（PG-LND201） | 本製品 | |
| PG-LND201 LAN ドライバ | 本ドライバ、LAN ドライバ | |
| Microsoft® Windows Server® 2003, Standard Edition | Windows Server 2003 | Windows |
| Microsoft® Windows Server® 2003, Enterprise Edition | | |
| Microsoft® Windows Server® 2003 R2, Standard Edition | | |
| Microsoft® Windows Server® 2003 R2, Enterprise Edition | | |
| Microsoft® Windows Server® 2003, Standard x64 Edition | Windows Server 2003 x64 | |
| Microsoft® Windows Server® 2003, Enterprise x64 Edition | | |
| Microsoft® Windows Server® 2003 R2, Standard x64 Edition | | |
| Microsoft® Windows Server® 2003 R2, Enterprise x64 Edition | | |
| Microsoft® Windows® 2000 Server | Windows 2000 Server | |
| Microsoft® Windows® 2000 Advanced Server | | |
| Red Hat® Enterprise Linux® ES (v.3 for x86) | Linux | |
| Red Hat® Enterprise Linux® AS (v.3 for x86) | | |
| Red Hat® Enterprise Linux® AS (v.4 for x86) | | |
| Red Hat® Enterprise Linux® ES (v.4 for x86) | | |
| Red Hat® Enterprise Linux® AS (v.4 for EM64T) | | |
| Red Hat® Enterprise Linux® ES (v.4 for EM64T) | | |
| Red Hat® Enterprise Linux® 5 (for x86) | | |
| Red Hat® Enterprise Linux® 5 (for Intel64) | | |
| PRIMERGY BX620 S3 サーバブレード | BX620 S3 サーバブレード | サーバブレード |
| PRIMERGY BX620 S4 サーバブレード | BX620 S4 サーバブレード | |
| PRIMERGY BX600 S3 シャーシ | シャーシ | |
| PRIMERGY BX600 S2 シャーシ | | |
| PRIMERGY BX600 スイッチブレード | スイッチブレード | |
| Catalyst Blade Switch 3040 | | |
| PRIMERGY BX600 ファイバーチャネル パススルーブレード | ファイバーチャネルパススルーブレード | |
| PRIMERGY BX600 ファイバーチャネル スイッチブレード（4Gbps）（PG-FCS103/PG-FCS102） | ファイバーチャネルスイッチブレード | |

# 安全上のご注意

本製品を安全にお使いいただくために、以降の記述内容を必ずお守りください。

## ■本製品の取り扱いについて

### ⚠警告

・機器を勝手に改造しないでください。火災・感電の原因となります。
・本製品に水をかけたり、濡らしたりしないでください。火災・感電の原因となります。

・近くで雷が発生した時は、本体の電源コードや本製品の外部接続コードを抜いてください。そのまま使用すると、雷によっては機器を破壊し、火災の原因となります。

### ⚠注意

・本製品は精密に作られていますので、高温・低温・多湿・直射日光など極端な条件での使用・保管は避けてください。
またカードを曲げたり、傷つけたり、強いショックを与えないでください。
故障・火災の原因となることがあります。

## ■リサイクルについて

本製品を廃棄する場合、担当営業員に相談してください。本製品は産業廃棄物として処理する必要があります。

# 梱包物の確認

お使いになる前に、次のものが梱包されていることをお確かめください。
万一足りないものがございましたら、担当営業員にご連絡ください。

- **LAN 拡張ボード**
- **保証書**
- **取扱説明書（本書）**
- **ネジ（3 本）**

J

Intel は、米国インテル社の登録商標です。
Microsoft、Windows、Windows Server は、米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。
Linux は、Linus Torvalds 氏の米国およびその他の国における登録商標あるいは商標です。
Red Hat および Red Hat をベースとしたすべての商標とロゴは、米国およびその他の国における Red Hat, Inc. の商標または登録商標です。
その他の各製品は、各社の商標、または登録商標です。
その他の各製品は、各社の著作物です。

All Rights Reserved, Copyright© FUJITSU LIMITED 2007

# 目次


**1 LAN 拡張ボードについて ..... 7**

1.1 概要 ..... 7

1.2 仕様 ..... 7

1.3 機能と特徴 ..... 8

**2 LAN 拡張ボードの取り付け ..... 17**

2.1 BX620 S3 ／ BX620 S4 サーバブレードへの取り付け方法 ..... 17

**3 LAN ドライバのインストール ..... 20**

3.1 ドライバソフトウェアのインストール方法 ..... 20

**4 Broadcom Gigabit Ethernet のチーム化サービス ..... 21**

4.1 Broadcom Gigabit Ethernet の概要 ..... 21

4.2 用語集 ..... 21

4.3 チーム化の概念 ..... 23

4.4 チーム化の仕組み ..... 34

4.5 チームタイプ ..... 37

4.6 各チームタイプと関連する各種機能の属性 ..... 40

4.7 チーム化とその他の高度なネットワークプロパティ ..... 42

4.8 全般的なネットワークに関する注意事項 ..... 45

4.9 イベントログのメッセージ ..... 55

**5 Broadcom Advanced Control Suite 2（BACS2） ..... 61**

5.1 BACS2 の概要 ..... 61

5.2 BACS2 のインストール方法 ..... 63

5.3 BACS2 の起動方法 ..... 67

5.4 BACS2 の設定 ..... 67

5.5 チームの設定 ..... 82

# 1　LAN 拡張ボードについて

この章では、本製品の特長、仕様について説明します。

## 1.1　概要

本製品は、BX620 S3 サーバブレードおよび BX620 S4 サーバブレード専用の LAN 拡張ボードです。
本製品は 1 ポートの LAN コントローラを 2 個搭載し、オンボード LAN とは完全に分離／独立した LAN 接続を提供します。外部へのアクセスは、シャーシのネットワークブレードスロット 3 またはネットワークブレードスロット 4（NET3 または NET4）に搭載するスイッチブレードなどを経由して行います。

**重要**

- 同一シャーシ内に、本製品を搭載したサーバブレードとファイバーチャネル拡張ボードを搭載したサーバブレードを混在させることはできません。
- ネットワークブレードスロット 3 またはネットワークブレードスロット 4（NET3 または NET4）にスイッチブレードを搭載する場合、ファイバーチャネルパススルーブレードやファイバーチャネルスイッチブレードの同時搭載はできません。

## 1.2　仕様

| 項目 | | 仕様 |
|---|---|---|
| 型名 | | PG-LND201 |
| ホストバス仕様 | インタフェース | PCI-Express（x4） |
| | データ転送速度 | 最大 1Gbps |
| | データ転送方式 | バスマスタ、DMA |
| 外部インタフェース | | 1000BASE-T Ethernet（SerDes）インタフェース |
| コントローラ LSI | | BCM 5708S |
| 適用機種 | | BX620S3 サーバブレード<br>BX620S4 サーバブレード |

J

# 1.3 機能と特徴

## 1.3.1 機能の説明

本製品は、新しいクラスのギガビットイーサネット（GbE）コンバージドネットワークインタフェースコントローラ（C-NIC）を搭載し、標準的なイーサネットネットワークで、高速化されたデータネットワーク、ストレージネットワーク、高性能クラスタリングを同時に実行できます。C-NIC は、次のようなデータセンターで使用される一般的なすべてのプロトコルで高速化を実現します。

・TCP を高速化する TCP Offload Engine（TOE）

**POINT**

- **SNP（Scalable Networking Pack）がインストールされた Windows Server 2003 に本製品を取り付けると、オフロードテクノロジーがサポートされます。**

Broadcom のチーム化ソフトウェアを使用すると、ロードバランスおよびフォルトトレランス機能を実現するために、ネットワークをバーチャル LAN（VLAN）に分割したり、複数のネットワークアダプタをチームにグループ化したりすることができます。チームに関する詳細は、「1.3.3 チームの機能」の「■ BASP（Broadcom Advanced Server Program）の概要」（→ P.10）を参照してください。VLAN に関しては、「1.3.4 仮想 LAN 機能」（→ P.14）を参照してください。Windows オペレーティングでチームの設定および VLAN の作成を行う方法については、「1.3.3 チームの機能」（→ P.10）を参照してください。

## 1.3.2 各種機能

本製品の機能を次に示します。

・TCP Offload Engine（TOE）
・シングルチップソリューション
  - 標準 Ethernet フレームサイズ（1518 バイト）
  - PCI Express v1.0A、x4
  - 完全高速パス TCP オフロード
  - ゼロコピー対応ハードウェア
・その他のパフォーマンス機能
  - TCP、IP、UDP チェックサム
  - TCP 区分化
・管理方法
  - Broadcom Advanced Control Suite 2 診断設定ソフトウェアスイート
  - PXE 2.0 仕様のサポート
  - SNMP MIB II、Ethernet に近い MIB、Ethernet MIB（IEEE 標準 802.3z、第 30 条）の統計
  - IPMI のサポート
・先進的なネットワーク機能
  - Jumbo frames（最大 9KB）。
  - 仮想 LAN
  - フローコントロール（IEEE 規格 802.3x）
  - LiveLink™（32/64 ビット Windows でサポートされています）
  - 論理リンクコントロール（IEEE 規格 802.2）
・レイヤー 2 優先順位符号化（IEEE802.1p）

・高速オンチップ RISC プロセッサ
・サービス分類（CoS）は 4 種類まで可能
・96KB フレームバッファメモリを内蔵
・128 ビットのハッシングハードウェア機能によりマルチキャストアドレスをサポート
・EM64T プロセッササポート

## ■ TCP Offload Engine（TOE）

TCP/IP プロトコルスイートは、インターネット、LAN、ファイル転送など、幅広い用途で転送サービスを提供するために使用されます。TCP/IP Offload Engine（TOE）がない場合、TCP/IP プロトコルスイートは、ホスト CPU 上で動作して、リソースの多くを消費するので、アプリケーションで使用できるリソースは大幅に減少します。本製品のネットワークコントローラを使用すると、TCP/IP の処理はハードウェアに移行されて CPU が解放されるため、アプリケーションの処理など重要なタスクにリソースを使用できるようになります。

本製品のネットワークコントローラの TOE 機能では、完全にオフロードされた TCP 接続を同時に 1024 まで確立できます。アダプタでの TOE サポートにより、オペレーティングシステムスタックの搭載を保護すると同時に、ホスト CPU の使用率を大幅に削減します。

## ■ Broadcom Advanced Control Suite 2

Broadcom のチーム化ソフトウェアのコンポーネントである Broadcom Advanced Control Suite 2（BACS2）は、統合型ユーティリティであり、システムにインストールされている各ネットワークアダプタに関する情報を提供します。

BACS2 では、各アダプタの詳細なテスト、診断、分析を実行できる上、プロパティ値の変更や各アダプタのトラフィック情報の表示も行えます。BACS2 は Windows でチームの設定および VLAN の追加に使用します。

## 1.3.3　チームの機能

### ■BASP（Broadcom Advanced Server Program）の概要

BASP（Broadcom Advanced Server Program）は、Windows Server 2003 または Windows 2000 Server に対応した、Broadcom のチーム化ソフトウェアです。BASP は BACS2 ユーティリティの一部として実行します。

BASP では、レイヤー 2 のチーム化のために、次の 4 タイプのチームがサポートされています。

・Smart Load Balancing（スマートロードバランス）およびフェイルオーバー
・リンク集約（802.3ad）
・通有中継（FEC/GEC）/802.3ad-Draft Static
・スマートロードバランス（SLB）（自動フォールバックはディスエーブル）

**POINT**

- Windows Server 2003 のビルトインブリッジングは、チーム化ソフトウェアの実行中に利用しないでください。

ネットワークアダプタのチーム化の概念については、「4.3 チーム化の概念」（→ P.23）を参照してください。

### ■ロードバランシングとフォルトトレランス

チーム化を行うことで、トラフィックのロードバランシングとフォルトトレランス（ネットワーク接続に失敗した場合に、アダプタの動作を冗長化すること）が実現できます。
1 台のシステムに複数のギガビットイーサネットネットワークアダプタが取り付けられているときは、仮想アダプタを作成することで、アダプタを複数のチームにグループ化できます。

1 つのチームは、2 ～ 8 つのネットワークインタフェースで構成でき、それぞれのインタフェースはプライマリインタフェースかスタンバイインタフェースとして指定できます。なお、スタンバイインタフェースは Smart Load Balancing™（スマートロードバランス）およびフェイルオーバーチームタイプでのみ使用可能で、1 つの SLB チームにはスタンバイインタフェースを 1 つだけ指定可能です。アダプタ、ケーブル、スイッチポート、またはスイッチ（チーム化されたアダプタが別のスイッチに取り付けられているもの）の不良のために、アダプタのチームメンバ通信でトラフィックが認識されない場合、負荷分散は再評価され、その他のチームメンバに再度割り当てられます。すべてのプライマリアダプタがダウンした場合は、ホットスタンバイアダプタがアクティブになります。このため、既存のセッションが維持され、ユーザへの影響はありません。

## ■チームタイプ

Windows Server 2003 および Windows 2000 Server で利用可能なチームのタイプは、次のとおりです。

・Smart Load Balancing（スマートロードバランス）およびフェイルオーバー
→「■ Smart Load Balancing™（スマートロードバランス）およびフェイルオーバー」（P.11）
・リンク集約（802.3ad）
→「■ リンク集約（802.3ad）」（P.12）
・通有中継（FEC/GEC）/802.3ad-Draft Static
→「■ 通有中継（FEC/GEC）/802.3ad-Draft Static」（P.12）
・スマートロードバランス（SLB）（自動フォールバックはディスエーブル）
→「■ スマートロードバランス（SLB）（自動フォールバックはディスエーブル）」（P.12）

**重要**

- ブレードサーバでは、リンク集約をサポートしていません。

## ■Smart Load Balancing™（スマートロードバランス）およびフェイルオーバー

Smart Load Balancing™ およびフェイルオーバーは、IP フローに基づくロードバランシングを Broadcom で実現します。この機能は、双方向で複数のアダプタ（チームメンバ）による IP トラフィックのバランシングをサポートします。このチームタイプでは、チーム内のすべてのアダプタは、個別の MAC アドレスを持っています。また、自動故障検出と、別のチームメンバまたはホットスタンバイメンバに対する動的フェイルオーバーが行われます。この処理は、レイヤー 3 プロトコル（IP、IPX、NetBEUI）からは独立しており、既存のレイヤー 2 スイッチとレイヤー 3 スイッチで実行されます。このチームタイプには、中継、リンク集約などのスイッチのコンフィギュレーションは必要ありません。

**POINT**

- SLB チームの設定時に LiveLink™ を有効にしない場合は、スイッチまたはポートでスパニングツリープロトコル（STP）を無効にしてください。これにより、フェイルオーバー時のスパニングツリーループ決定によるダウンタイムが最低限に抑えられます。LiveLink™ は、このような問題を可能な限り回避します。
- IPX はチームの送信側のみでバランス取りします。他のプロトコルの場合、バランス取りはプライマリアダプタに限定されます。
- 一方のチームメンバが 1000Mbit/ 秒でリンクされ、もう一方のチームメンバが 100Mbit/ 秒でリンクされている場合、ほとんどのトラフィックは 1000Mbit/ 秒のチームメンバによって処理されます。

## ■ リンク集約（802.3ad）

このモードはリンク集約をサポートし、IEEE802.3ad（LACP）仕様に準拠しています。コンフィギュレーションソフトウェアを使用すると、任意のチーム内でどのアダプタに分配するかを動的に設定できます。リンクのパートナーが 802.3ad リンクに正しく設定されていない場合は、エラーが検出され記録されます。このモードでは、チーム内のすべてのアダプタが同じ MAC アドレスの受信パケットに設定されます。アウトバウンドのロードバランシングスキームは、BASP ドライバにより決定されます。インバウンドパケットのロードバランシングスキームは、チームのリンクパートナーにより決定されます。このモードでは、少なくとも 1 つのリンクパートナーがアクティブモードとされている必要があります。

**重 要**

- ブレードサーバでは、リンク集約（802.3ad）をサポートしていません。

## ■ 通有中継（FEC/GEC）/802.3ad-Draft Static

通有中継（FEC/GEC）/802.3ad-Draft Static チームタイプは、同じ MAC アドレスに対するパケットを受信するように設定する点で、リンク集約（802.3ad）チームタイプと非常に似ています。ただし、通有中継（FEC/GEC）/802.3ad-Draft Static チームタイプでは、LACP またはマーカープロトコルはサポートされません。アダプタのリンクパートナーが独自仕様のトランキング方法をサポートするよう静的に設定されている環境のときに、このチームタイプの使用が可能です。たとえば、Lucent の OpenTrunk や Cicso の FEC（Fast EtherChannel）で使用可能です。基本的に、このチームタイプは、リンク集約（802.3ad）チームタイプの簡易バージョンといえます。リンク集約制御プロトコル（LACP）には複数の仕様が存在するため、この方法はとても簡易的なものです。他のチームタイプと同様に、チームの作成、およびさまざまなチームに対する物理的なアダプタの割り当ては、ユーザーコンフィギュレーションソフトウェアで静的に行います。
通有中継（FEC/GEC/802.3ad-Draft Static）チームタイプは、受発信のトラフィックのロードバランシングとフェイルオーバーをサポートしています。

## ■ スマートロードバランス（SLB）（自動フォールバックはディスエーブル）

SLB（自動フォールバックはディスエーブル）チームタイプは、Smart Load Balancing™ およびフェイルオーバーチームタイプと同一です。ただし、スタンバイメンバがアクティブで、プライマリメンバが再びオンラインになった場合、チームはプライマリメンバに切り替えずに、スタンバイメンバをそのまま使用するところが異なります。

チーム内のプライマリインタフェースは、すべてトラフィックの一部の送受信などのロードバランシング動作に利用されます。スタンバイインタフェースは、すべてのプライマリインタフェースがリンク切断された場合に代用されます。

フェイルオーバーのチーム化を行うと、万が一ネットワーク接続に失敗した場合に、アダプタの動作が冗長化されます（フォルトトレランス）。アダプタ、ケーブル、スイッチポートなどの不良によりチーム内のプライマリアダプタの接続が切断された場合、セカンダリチームメンバがアクティブになり、本来プライマリアダプタに割り当てられていた受発信トラフィックをリダイレクトします。セッションは継続され、ユーザに影響が及ぶことはありません。

## ■ Smart Load Balancing™ およびフェイルオーバー /SLB（自動フォールバックはディスエーブル）チームタイプの制限事項

Smart Load Balancing™ （SLB：スマートロードバランス）は、プロトコル固有のスキームです。IP、IPX、NetBEUI プロトコルでのサポート状況を次に示します。

| オペレーティングシステム | フェイルオーバー：フェイルバック－ Broadcom 全製品 | | | フェイルオーバー：フェイルバック－ 非 Broadcom 製品 | | | 負荷バランス－ Broadcom 全製品 | | | 負荷バランス－ 非 Broadcom 製品 | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| プロトコル | IP | IPX | Net BEUI | IP | IPX | Net BEUI | IP | IP X | NetBE UI | IP | IPX | Net BEUI |
| Windows Server 2003 | Y | Y | N | Y | N | N | Y | Y | N | Y | N | N |
| Windows Server 2003（SNP） | Y | Y | N | Y | N | N | Y | Y | N | Y | N | N |
| Windows 2000 Server | Y | Y | Y | Y | N | N | Y | Y | N | Y | N | N |

Y：サポートあり、N：サポートなし

Smart Load Balancing™ チームタイプは、スイッチポートを特殊な中継モードに設定しなくても、すべてのイーサネットスイッチで動作します。IP トラフィックのみ、発信・戻りの双方向でロードバランスされます。IPX トラフィックは、発信方向のみでロードバランスが行われます。その他のプロトコルパケットは、1 つのプライマリインタフェースのみで送受信されます。非 IP トラフィックのフェイルオーバーは、ネットワークアダプタ以外ではサポートされていません。通有中継チームタイプでは、何らかのポート中継モード（たとえば、Cisco の Gigabit EtherChannel などの各スイッチメーカーのリンク集約モード）をサポートするイーサネットスイッチが必要になります。通有中継チームタイプはプロトコルに依存せず、すべてのトラフィックはロードバランスが行われ、フォルトトレランスの対象になります。

**POINT**

- **チームの設定時に LiveLink™ を有効にしない場合は、スイッチでスパニングツリープロトコル（STP）を無効にしてください。これにより、フェイルオーバーの実行時にスパニングツリーのループが決定されるまでのダウンタイムを最低限に抑えることができます。LiveLink™ は、このような問題を可能な限り回避します。**

## ■ LiveLink™

LiveLink™ は、BASP の機能の 1 つで、Smart Load Balancing™ チームタイプでのみ動作します。LiveLink™ は、スイッチで発生したリンクロスを検出し、リンクが有効になっているチームメンバのみのトラフィックをルーティングします。この機能は、チーム化ソフトウェアでも使用することができます。チーム化ソフトウェアは、各チームメンバからリンクパケットを発行して、1 つまたは複数の特定ネットワークデバイスのプローブ（検査）を行います。プローブ対象は、リンクパケットを受信すると応答を返します。チームメンバが一定時間内に応答を検出しない場合、リンクは損失しており、チーム化ソフトウェアはそのチームメンバとのトラフィックの送受信を中断します。その後、そのチームメンバがプローブ対象からの応答を検出した場合、リンクは復元され、チーム化ソフトウェアはそのチームメンバとのトラフィックの送受信を自動的に再開します。LiveLink™ は、TCP/IP でのみ動作します。

LiveLink™ は、32/64 ビット Windows でサポートされています。Linux のチャネル結合に備わっている同様の機能については、チャネル結合のドキュメント（http://www.redhat.com/docs/manuals/enterprise/RHEL-3-Manual/ref-guide/s1-modules-ethernet.html）を参照してください。

### ■ チーム化および Large Send Offload（大量送信オフロード）/ Checksum Offload（チェックサムオフロード）のサポート

Large Send Offload（LSO、大量送信オフロード）と Checksum Offload（チェックサムオフロード）は、チームのすべてのメンバで両方のオフロードがサポートされ、設定されている場合にのみ、そのチームに対して自動的に有効となります。

## 1.3.4　仮想 LAN 機能

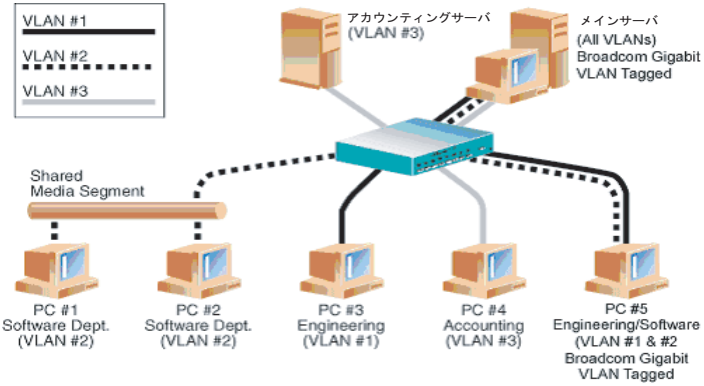
### ■ 仮想 LAN（Virtual LAN）の概要

仮想 LAN（VLAN）を利用すると、物理的な LAN を論理的な区域に分割し、ワークグループの論理的なセグメントを作成できます。これにより各論理セグメントごとにセキュリティポリシーを設定することが可能になります。定義済みの VLAN は、そのトラフィックや同報通信がその他の VLAN から分離されるため、それぞれが独自の分離されたネットワークとして機能します。これにより各論理グループ内の帯域幅の効率が向上します。サーバ上の 1 つの Broadcom アダプタには、最大 64 個（タグ付けされたもの 63 個、タグ付けされていないもの 1 個）までの VLAN が定義できます。定義できる数はシステム内で利用できるメモリ数により異なります。

チームには複数の VLAN を追加し、異なる VLAN ID をもつ複数の VLAN を許可できます。バーチャルアダプタが追加されたそれぞれの VLAN について作成されます。

VLAN は通常、独立した同報通信のドメインを作成したり、IP サブネットを分離するとき利用しますが、サーバ本体には同時に複数の VLAN を与えておくと便利です。ポート別またはチーム別に複数の VLAN がサポートできます。このためネットワークのコンフィギュレーションがとてもフレキシブルになります。

・タグ付けされた複数の VLAN をサポートするサーバの例



前の図は、VLAN を使用するネットワークの例を示しています。このネットワーク例では、物理 LAN は 1 つのスイッチ、2 つのサーバ、5 つのクライアントで構成されています。LAN は論理的に 3 つの異なる VLAN に組織化されます。VLAN はそれぞれ異なる IP サブネットを代表します。このネットワークの機能について、次に示します。

・VLAN ネットワークのトポロジー例

| コンポーネント | 説明 |
|---|---|
| VLAN #1 | メインサーバ、PC #3、PC #5 で構成される IP サブネットです。このサブネットはエンジニアリンググループを表します。 |
| VLAN #2 | メインサーバ、共有メディアセグメント経由の PC #1、PC#2、および PC #5 を含みます。この VLAN はソフトウェア開発グループです。 |
| VLAN #3 | メインサーバ、アカウンティングサーバ、PC #4 を含みます。この VLAN はアカウンティンググループです。 |
| メインサーバ | 最も頻繁に使用されるサーバで、すべての VLAN と IP サブネットからアクセスする必要があります。メインサーバには Broadcom アダプタがインストールされています。3 つの IP サブネットには、1 つの物理アダプタインタフェースでアクセスします。サーバはスイッチポートの 1 つに取り付け、VLAN#1、#2、#3 に構成します。2 つのアダプタと接続されたスイッチポートのタギングはオンにします。この両デバイスのタグ付けされた VLAN の容量のために、サーバはネットワーク内では 3 つの IP サブネットすべてで通信を行うことができますが、同報通信分離を維持してください。 |
| アカウンティングサーバ | VLAN #3 のみで利用可能です。アカウンティングサーバは VLAN #1 と VLAN #2 上のすべてのトラフィックから遮断されます。サーバに接続されたスイッチポートのタギングはオフにします。 |
| PC #1 および PC #2 | 共有メディアハブに接続し、次にスイッチに接続します。PC #1 と PC #2 は VLAN #2 のみに属し、論理的にはメインサーバと PC #5 と同じ IP サブネットにあります。このセグメントに接続されたスイッチポートのタギングはオフになります。 |
| PC #3 | VLAN #1 と PC #3 のメンバは、メインサーバと PC #5 のみ通信できます。PC #3 のスイッチポート上ではタギングは有効にできません。 |
| PC #4 | VLAN #3 と PC #4 のメンバはサーバのみ通信できます。PC #4 のスイッチポート上ではタギングは有効にできません。 |
| PC #5 | VLAN #1、#2 のメンバと PC #5 には Broadcom アダプタがインストールされています。アダプタはスイッチポート #10 に接続されます。両方のアダプタとスイッチポートは VLAN #1 と VLAN #2 用に設定され、タギングが有効となります。 |

**POINT**

- **VLAN のタギングは、他のスイッチに対する中継リンクを作成するスイッチポート上、または Broadcom アダプタを使用しているサーバやワークステーションといったタグ付け可能なエンドステーション以外では有効にする必要はありません。**

## ■チームに VLAN を追加する

1 つのチームあたり、64 個の VLAN がサポートできます（タグ付けされたもの 63 個、タグ付けされていないもの 1 個）。 1 つのアダプタ上に複数の VLAN がある場合、アダプタが 1 つしかないサーバでは、複数の IP サブネット上に 1 つの論理プレゼンスしか与えられません。 1 つのチームに複数の VLAN がある場合は、複数の IP サブネットに 1 つの論理プレゼンスを与え、ロードバランシングとフェイルオーバーによる利点を生かすことができます。チームに VLAN を追加する手順について、Windows の場合は「5.5 チームの設定」（→ P.82）を参照してください。

**POINT**

- フェイルオーバーチームのメンバとなっているアダプタも VLAN のサポートを設定できます。Intel LOM がフェイルオーバーチームのメンバである場合、Intel LOM では VLAN がサポートされないため、VLAN をチームに設定することはできません。

# 2　LAN 拡張ボードの取り付け

この章では、本製品のサーバブレードへの取り付け方法について説明します。

## ⚠ 警告

・取り付けや取り外しを行うときは、サーバブレードをシャーシから取り外してください。感電の原因となります。
シャーシからの取り外し方法は、『シャーシ ハードウェアガイド』を参照してください。

## ⚠ 注意

・内蔵オプションは、基板や半田づけした部分がむきだしになっています。これらの部分は、人体に発生する静電気によって損傷を受ける場合があります。
取り扱う前に、サーバ本体の金属部分に触れて人体の静電気を放電してください。
・基板表面や半田づけの部分に触れないように、金具の部分や基板の縁を持つようにしてください。
・本製品は静電気の影響を受けやすいので、伝導パッドなどの上に置くか、取り扱う直前まで梱包袋に入れておいてください。

## 2.1　BX620 S3 ／ BX620 S4 サーバブレードへの取り付け方法

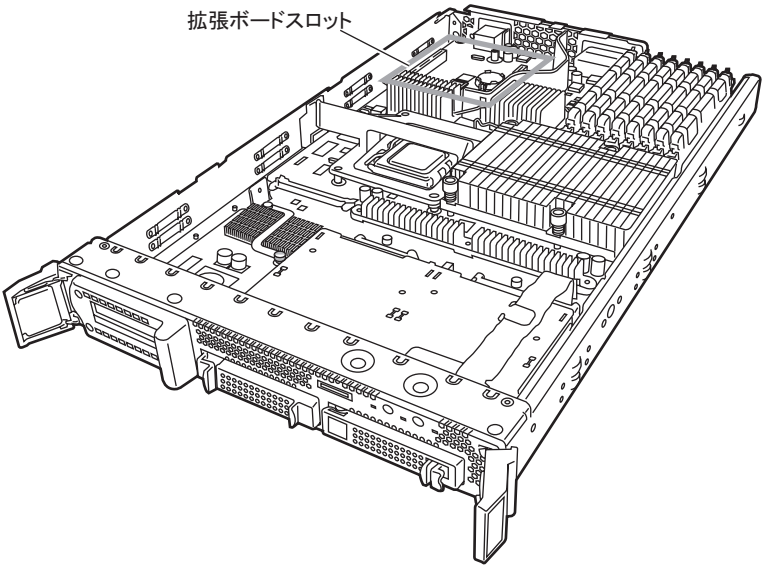
**POINT**

- LAN 拡張ボードを外部 LAN（装置）に接続するには、シャーシのネットワークブレードスロット 3 またはネットワークブレードスロット 4（NET3 または NET4）にスイッチブレードまたは LAN パススルーブレードを搭載する必要があります。

J

## 2.1.1 LAN 拡張ボードの取り付け位置

BX620 S3 ／ BX620 S4 サーバブレードの拡張ボードスロットに取り付けます。




## 2.1.2 LAN 拡張ボード取り付け手順

**1 LAN 拡張ボードを取り付けるサーバブレードの電源を切ります。**
→『シャーシ ハードウェアガイド 3.3 電源を切る』

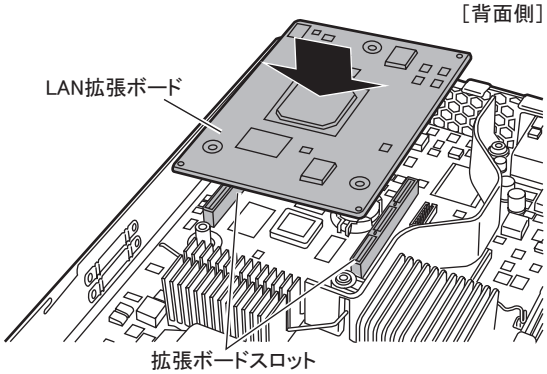
**2 シャーシの金属部分に触れて人体の静電気を放電します。**

**3 サーバブレードを、シャーシから取り外します。**
→『シャーシ ハードウェアガイド 4.2 サーバブレードの取り付け』

**4 トップカバーを取り外します。**
→『 サーバブレード ユーザーズガイド 7.2 トップカバーの取り付け／取り外し』

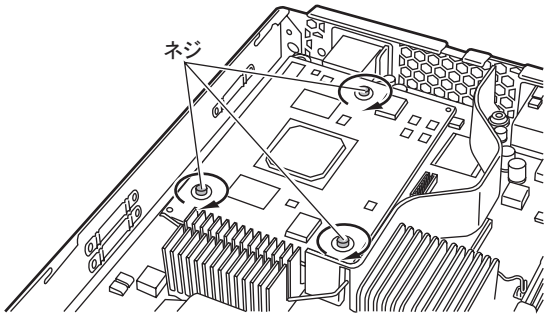
### 5 LAN 拡張ボードを取り付けます。

LAN 拡張ボードが完全にスロットに差し込まれたことを確認してください。




### 6 LAN 拡張ボードをネジで固定します。

LAN 拡張ボードを、ボードに添付のネジ（3 本）で固定します。




### 7 トップカバーを取り付けます。

→『 サーバブレード ユーザーズガイド 7.2 トップカバーの取り付け／取り外し』

### 8 サーバブレードをシャーシに取り付けます。

→『シャーシ ハードウェアガイド 4.2 サーバブレードの取り付け』

J

# 3 LAN ドライバのインストール

この章では、LAN ドライバのインストール方法について説明します。

## 3.1 ドライバソフトウェアのインストール方法

**POINT**

- LAN ドライバは、次の中から入手してインストールしてください。
  ・BX620 S4 サーバブレードに添付されている ServerStart CD-ROM 内の LAN ドライバ
  ・弊社のインターネット情報ページ（http://primeserver.fujitsu.com/primergy/）に公開されている LAN ドライバ
  なお、上記より新しい LAN ドライバを使用する場合は、そのドライバに添付されている取扱説明書またはヘルプファイルを参照してください。
- PRIMERGY サーバ上では、Broadcom 社のオンラインサービスからダウンロードした LAN ドライバを使用しないでください。
- ドライバソフトウェアをインストールする前に、Windows が最新サービスパックにより最新バージョンに更新されていることを確認してください。
- TCP/IP Offload Engine（TOE）を使用する場合は、Windows Server 2003 の Scalable Networking Pack（SNP）が必要です。

### 3.1.1 LAN ドライバのインストール

インストーラは、Windows Server 2003 用 SNP がマシンにインストールされているかどうかを検出します。インストールされている場合、インストーラは、TOE に必要な NDIS 5.2 ドライバをインストールします。Windows Server 2003 用 SNP マシンにインストールされていない場合、NDIS 5.1 ドライバをインストールして、TOE を使用することはできません。

**1 ダウンロードした LAN ドライバのあるフォルダを開く、または Server Start Disc1 CD-ROM をセットします。**

**2 次の EXE を実行します。**

- Windows Server 2003 x64 の場合
  ¥DRIVERS¥LAN¥Broadcom¥Ext¥W2K3x64¥DrvInst¥setup.exe
- Windows Server 2003 の場合
  ¥DRIVERS¥LAN¥Broadcom¥Ext¥W2K3¥DrvInst¥setup.exe
- Windows Server 2000 の場合
  ¥DRIVERS¥LAN¥Broadcom¥Ext¥W2K¥DrvInst¥setup.exe

**3 ［Next］をクリックします。**

ドライバのインストールが開始されます。

**4 ［Finish］をクリックします。**

**5 CD-ROM を取り出し、サーバブレードを再起動します。**

# 4 Broadcom Gigabit Ethernet のチーム化サービス

この章では、ネットワークチーム化サービスを使用する際の技術および注意事項について説明します。

## 4.1 Broadcom Gigabit Ethernet の概要

このサービスは、Broadcom ソフトウェアによって提供されます。Broadcom のチーム化サービスの目的は、複数のアダプタからなるチーム全体にフォルトトレランスとリンク集約を提供することです。本章の内容は、IT プロフェッショナルが、ネットワークフォルトトレランスとロードバランシングを必要とするシステムアプリケーションを導入しトラブルシューティングする際に役立ちます。

## 4.2 用語集

| 項目 | 定義 |
|---|---|
| ARP | Address Resolution Protocol：アドレス解決プロトコル |
| BACS | Broadcom Advanced Control Suite |
| BASP | Broadcom Advanced Server Program（中間ドライバ） |
| DNS | Domain Name Service：ドメインネームサービス |
| G-ARP | Gratuitous Address Resolution Protocol：無償アドレス解決プロトコル |
| 通有中継（FEC/GEC）/802.3ad-Draft Static | スイッチ依存型のロードバランシングおよびフェイルオーバーチームタイプで、中間ドライバが発信トラフィックを管理し、スイッチが受信トラフィックを管理します。 |
| HSRP | Hot Standby Router Protocol：ホットスタンバイルータープロトコル |
| ICMP | Internet Control Message Protocol：インターネット制御メッセージプロトコル |
| IGMP | Internet Group Management Protocol：インターネットグループ管理プロトコル |
| IP | Internet Protocol：インターネットプロトコル |
| LACP | Link Aggregation Control Protocol：リンク集約制御プロトコル |
| リンク集約（802.3ad） | LACP を使用するロードバランシングおよびフェイルオーバーチームタイプで、中間ドライバが発信トラフィックを管理し、スイッチが受信トラフィックを管理します。 |
| LOM | LAN on Motherboard：マザーボード内蔵 LAN |

| 項目 | 定義 |
| --- | --- |
| MAC | Media Access Control：メディアアクセス制御 |
| NDIS | Network Driver Interface Specification：ネットワークドライバインタフェース仕様 |
| NLB | Network Load Balancing：ネットワーク負荷分散（Microsoft） |
| PXE | Preboot Execution Environment：プリブート実行環境 |
| RAID | redundant array of inexpensive disks：低価格ディスクの冗長アレイ |
| Smart Load Balancing（スマート ロード バランス）およびフェイルオーバー | スイッチ独立型のフェイルオーバーチームタイプで、フェイルオーバーイベント（リンクロスなど）が発生するまではプライマリチームメンバがすべての発受信トラフィックを処理し、スタンバイチームメンバはアイドルになります。中間ドライバ（BASP）が受信／発信トラフィックを管理します。 |
| Smart Load Balancing（SLB） | スイッチ独立型のロードバランシングおよびフェイルオーバーチームタイプで、中間ドライバが発信／受信トラフィックを管理します。 |
| TCP | Transmission Control Protocol：伝送制御プロトコル |
| UDP | User Datagram Protocol：ユーザーデータグラムプロトコル |
| WINS | Windows name service：Windows ネームサービス |
| WLBS | Windows Load Balancing Service：Windows 負荷分散サービス |

# 4.3　チーム化の概念

記憶デバイスでは、RAID テクノロジーを使用して個々のハードドライブをグループ化します。スイッチポートは、Cisco Gigabit EtherChannel、IEEE 802.3ad リンク集約、Bay Network Multilink Trunking、および Extreme Network Load Sharing などのテクノロジーを使用してグループ化できます。サーバのネットワーク インタフェースは、仮想アダプタと呼ばれる物理ポートのチームにグループ化できます。

## 4.3.1　チーム化とネットワークアドレスについて

### ■ネットワークアドレス指定

チーム化の動作方法を理解するには、イーサネットネットワークにおけるノード通信の動作方法を理解することが重要です。ここでは、読者に IP およびイーサネットネットワーク通信の基礎知識があることを前提とし、イーサネットネットワークで使用されるネットワークアドレス指定の概念について説明します。

コンピュータシステムのようなホストプラットフォームのイーサネットネットワークインタフェースは、どれもグローバルに一意なレイヤー 2 アドレスを 1 つと、グローバルに一意なレイヤー 3 アドレスを少なくとも 1 つ必要とします。OSI モデルで定義されているように、レイヤー 2 はデータリンクレイヤーで、レイヤー 3 はネットワークレイヤーです。レイヤー 2 アドレスはハードウェアに割り当てられ、多くの場合 MAC アドレスまたは物理アドレスと呼ばれます。このアドレスは工場出荷時にあらかじめプログラムされ、ネットワークインタフェースカードの NVRAM、または内蔵 LAN インタフェース用のシステムマザーボードの NVRAM に格納されます。レイヤー 3 アドレスはプロトコルアドレスまたは論理アドレスと呼ばれ、ソフトウェアスタックに割り当てられます。レイヤー 3 プロトコルの例としては、IP や IPX が挙げられます。また、レイヤー 4（トランスポートレイヤー）では Telnet や FTP などのネットワーク上位プロトコルごとにポート番号を使用します。これらのポート番号は、アプリケーション全体のトラフィックフローを識別するのに使用されます。IP アドレスと TCP ポート番号の組み合わせは、ソケットと呼ばれます。

イーサネットデバイスは、IP アドレスではなく MAC アドレスを使用して他のイーサネットデバイスと通信します。ただし、大部分のアプリケーションは、WINS や DNS などのネーミングサービスによって IP アドレスに変換されるホスト名で動作します。そのため、IP アドレスに割り当てられている MAC アドレスの識別方法が必要です。IP ネットワークの ARP（Address Resolution Protocol）はこのメカニズムを提供します。IPX の場合、MAC アドレスはネットワークアドレスの一部なので ARP は不要です。ARP は、ARP 要求および ARP 応答フレームを使用して搭載されます。ARP 要求は一般的にブロードキャストアドレスに送信され、ARP 応答は一般的にユニキャストトラフィックとして送信されます。ユニキャストアドレスは、単一の MAC アドレスまたは単一の IP アドレスに対応します。ブロードキャストアドレスは、ネットワーク上のすべてのデバイスに送信されます。

### ■チーム化とネットワークアドレス

アダプタのチームは、単一の仮想ネットワークインタフェースとして機能し、チーム化されていないアダプタのネットワークデバイスと同じように見えます。仮想ネットワークアダプタは、単一のレイヤー 2 アドレスと 1 つまたは複数のレイヤー 3 アドレスを通知します。チーム化ドライバは、初期化の際に、チームを構成する物理アダプタのいずれかから、チーム MAC アドレスとなる MAC アドレスを 1 つ選択します。一般的にこのアドレスは、ドライバが最初に初期化するアダプタから取得されます。チームを管理しているシステムは、ARP 要求を受信すると、チーム内の物理アダプタの中から MAC アドレスを 1 つ選択して、ARP 応答のソース MAC アドレスとして使用します。Windows では、IPCONFIG/all コマンドは個々の物理アダプタではなく仮想アダプタの IP アドレスと MAC アドレスを表示します。プロトコル IP アドレスは、個々の物理アダプタではなく仮想ネットワークインタフェースに割り当てられます。

スイッチ独立型のチーム化モードの場合、データ伝送時には、仮想アダプタを構成するすべての物理アダプタが、物理アダプタに割り当てられている一意の MAC アドレスを使用します。すなわち、チーム内の各物理アダプタで送信されるフレームは、一意の MAC アドレスを使用して IEEE に準拠する必要があります。ARP キャッシュエントリが、受信フレームからではなく、ARP 要求および ARP 応答からのみ情報を得ることに注意することが重要です。

## 4.3.2 チームタイプ

利用可能なチームタイプを次に示します。

| チームタイプ | スイッチ依存型 (*1) | スイッチに Link Aggregation Control Protocol のサポートが必要 | ロードバランシング | フェイルオーバー |
|---|---|---|---|---|
| Smart Load Balancing（スマートロードバランス）およびフェイルオーバー | − | − | ○ | ○ |
| スマートロードバランス（SLB）（自動フォールバックはディスエーブル） | − | − | ○ | ○ |
| リンク集約（802.3ad）(*2) | ○ | ○ | ○ | ○ |
| 通有中継（FEC/GEC）/ 802.3ad-Draft Static | ○ | − | ○ | ○ |

*1）スイッチが特定のチームタイプをサポートしている必要があります。
*2）ブレードサーバでは、リンク集約をサポートしていません。

## ■Smart Load Balancing（スマートロードバランス）およびフェイルオーバー

Smart Load Balancing™ およびフェイルオーバーチームタイプは、ロードバランシング用に設定されている場合はロードバランシングとフェイルオーバーの両方を提供し、フォルトトレランス用に設定されている場合にはフェイルオーバーのみを提供します。このチームタイプは、どのイーサネットスイッチでも動作し、スイッチのトランキング設定は不要です。チームは、複数の MAC アドレスおよび 1 つまたは複数の IP アドレスを通知します（セカンダリ IP アドレスを使用している場合）。チーム MAC アドレスは、「Load Balance メンバ」のリストから選択されます。システムで ARP 要求が受信されると、ソフトウェアネットワーキングスタックは常に ARP 応答とチーム MAC アドレスを送信します。ロードバランシングプロセスを開始するには、チーム化ドライバでソース MAC アドレスをいずれかの物理アダプタと一致するように変更して、この ARP 応答を修正します。

Smart Load Balancing は、レイヤー 3/ レイヤー 4、IP アドレスと TCP/UDP ポート番号に基づいて、伝送と受信の両方のロードバランシングを有効にします。すなわち、ロードバランシングはバイトまたはフレームレベルではなく、TCP/UDP セッションベースで実行されます。この方法は、同じソケットの通信に属するフレームを順序正しく配信し続けるために必要です。ロードバランシングは、2 ～ 8 個のポートでサポートされます。これらのポートには、アドインアダプタや LAN on Motherboard（LOM）デバイスの組み合わせが含まれます。伝送のロードバランシングは、発信元および宛先の IP アドレスと TCP/UDP ポート番号を使用してハッシュテーブルを作成することにより実現されます。発信元および宛先の IP アドレスと TCP/UDP ポート番号の組み合わせが同じ場合には、通常同じハッシュインデックスが作成されるため、チーム内の同じポートを指し示すことになります。指定されたソケットのすべてのフレームを搬送するようにポートが選択されている場合、チーム MAC アドレスではなく、物理アダプタの一意の MAC アドレスがフレームに含められます。これは、IEEE802.3 規格に準拠するために必要です。2 つのアダプタで同じ MAC アドレスを使用して伝送した場合、スイッチで処理できない MAC アドレスの重複状態が発生します。

受信のロードバランシングは、各クライアントのユニキャストアドレスを ARP 要求の宛先アドレスとして使用して（Directed ARP とも呼ばれる）、クライアント別に無償 ARP を送信することにより、中間ドライバで実現されます。これはクライアントロードバランシングと見なされ、トラフィックロードバランシングとはみなされません。中間ドライバは、SLB チーム内の物理アダプタ間で深刻なロードインバランスを検出すると、受信フレームを再分配するために G-ARP を生成します。中間ドライバ（BASP）は ARP 要求に応答しません。ソフトウェアプロトコルスタックが必要な ARP 応答を提供するだけです。受信のロードバランシングは、チームインタフェースでシステムに接続しているクライアントの数と相関関係にあります。

SLB の受信のロードバランシングは、チーム内の物理ポート全体でクライアントマシンの受信トラフィックのロードバランスを行おうとします。修正された G-ARP を使用して、送信者の物理アドレスとプロトコルアドレスに含まれるチーム IP アドレスの別の MAC アドレスを通知します。この G-ARP は、対象の物理アドレスとプロトコルアドレスのそれぞれに、クライアントマシンの MAC アドレスと IP アドレスを使用するユニキャストです。これにより、対象クライアントはその ARP キャッシュを、チーム IP アドレスへの新しい MAC アドレスマップで更新します。G-ARP はブロードキャストではありません。なぜなら、すべてのクライアントが同じポートにそのトラフィックを送信することになるからです。結果として、クライアントロードバランシングで得られる利点はなくなり、フレーム配信の順序が狂う可能性があります。この受信のロードバランシングのスキームは、すべてのクライアントとチーム化されたシステムが同じサブネットまたはブロードキャストドメインにある限り作用します。

クライアントとシステムが別のサブネットにあり、受信トラフィックがルーターを越えなければならない場合、システムに向かう受信トラフィックはロードバランスされません。中間ドライバで IP フローを搬送するよう選択された物理アダプタは、すべてのトラフィックを搬送します。ルーターはチーム IP アドレスにフレームを送信するときに、ARP 要求をブロードキャストします（ARP キャッシュにない場合）。サーバソフトウェアスタックはチーム MAC アドレスを使用して ARP 応答を生成しますが、中間ドライバがその ARP 応答を修正して特定の物理アダプタに送信し、そのセッションのフローを確立します。

これは、ARP がルーターブルプロトコルではないためです。ARP には IP ヘッダがありません。そのため、ルーターまたはデフォルトゲートウェイには送信されません。ARP はローカルサブネットプロトコルに過ぎません。さらに、G-ARP はブロードキャストパケットではないため、ルーターはそれを処理せず、それ自身の ARP キャッシュも更新しません。

ルーターが別のネットワークデバイス向けの ARP を処理するのは、代理 ARP が有効になっていて、ホストにデフォルトゲートウェイがない場合のみです。このような状態は非常にまれであり、大部分のアプリケーションにはお勧めできません。
ルーターを経由する伝送トラフィックはロードバランスされます。これは、伝送のロードバランシングが発信元および宛先の IP アドレスと TCP/UDP ポート番号に基づいているためです。ルーターでは発信元と宛先の IP アドレスが変更されないため、ロードバランシングのアルゴリズムは意図したとおりに動作します。

HSRP（Hot Standby Routing Protocol）のルーターの設定では、アダプタチーム内の受信のロードバランシングは発生しません。一般的に HSRP では、2 つのルーターが 1 つのルーターとして動作して、仮想 IP アドレスと仮想 MAC アドレスを通知します。1 つの物理ルーターがアクティブインタフェースになっているときには、もう片方がスタンバイになります。HSRP では（ホストノードにそれぞれ異なるデフォルトゲートウェイを使用して）HSRP グループの複数のルーターに共有ノードをロードすることもできますが、常にチームのプライマリ MAC アドレスを示します。

## ■スマートロードバランス（SLB）（自動フォールバックはディスエーブル）

このチームタイプは、スマートロードバランスおよびフェイルオーバーチームタイプと同一です。ただし、スタンバイメンバがアクティブな状態であり、プライマリメンバが動作を再開した場合、チームはプライマリメンバに切り替えずにスタンバイメンバをそのまま使用するところが異なります。このチームは、ネットワークケーブルが外されてネットワークアダプタに再接続されたときにのみサポートされます。アダプタがデバイスマネージャまたはホットプラグ PCI を介して取り外し／取り付けられた場合にはサポートされません。

チームに割り当てられたプライマリアダプタが無効にされた場合、チームは自動フォールバックが発生する Smart Load Balancing（スマートロードバランス）およびフェイルオーバーチームタイプとして機能します。

## ■リンク集約（IEEE 802.3ad LACP）

リンク集約は、Link Aggregation Control Protocol（LACP）を使用してチームを構成するポートをネゴシエートすることを除けば、通有中継と似ています。チームを使用できるようにするには、リンクの両端で LACP を有効にする必要があります。LACP がリンクの両端で利用可能になっていない場合、802.3ad は、リンクの両端がリンクアップ状態であることのみを要求する手動集約を提供します。手動集約は LACP メッセージ交換を実行せずにメンバリンクをアクティブ化するため、LACP ネゴシエートリンクと同程度に堅固で信頼できるとみなすことはできません。LACP は、どのメンバリンクが集約可能であるかを自動的に判断して、それらを集約します。リンク集約用の物理リンクの追加と削除を制御して、フレームが失われたり複製されたりしないようにします。集約リンクメンバの削除は、LACP 対応の集約リンクに対して、オプションとして使用可能なマーカープロトコルで提供されます。

リンク集約グループは、中継内のすべてのポートに対して単一の MAC アドレスを通知します。集約先の MAC アドレスは、グループを構成するいずれかの MAC アドレスである可能性があります。LACP とマーカープロトコルは、マルチキャスト宛先アドレスを使用します。

リンク集約制御機能は集約されるリンクを特定して、システムの集約機能にポートをバインドし、状況を監視して集約グループに変更が必要かどうかを判断します。リンク集約は複数のリンクの個々の能力を合わせて、高性能の仮想リンクを形成します。LACP トランク内のリンクの障害または交換で、接続性が失われることはありません。中継内の残りのリンクにトラフィックがフェイルオーバーされるだけです。

**重要**

- ブレードサーバでは、リンク集約をサポートしていません。

### ■通有中継

通有中継は、リンクの両端（サーバインタフェースとスイッチポート）でポートの設定を必要とするスイッチ支援のチームタイプです。これは、Cisco Fast EtherChannel または Gigabit EtherChannel と呼ばれます。さらに通有中継は、Extreme Networks Load Sharing および Bay Networks のような他のスイッチ OEM や、IEEE 802.3ad リンク集約の静的モードによる同様の搭載をサポートします。このモードでは、プロトコルスタックが ARP 要求に応答するときに、チームは 1 つの MAC アドレスと 1 つの IP アドレスを通知します。また、チーム内の各物理アダプタは、フレーム伝送時に同じチーム MAC アドレスを使用します。これが可能になるのは、リンクの反対側の端にあるスイッチがチームモードを認識して、チーム内のすべてのポートによる単一 MAC アドレスの使用を処理するからです。スイッチの転送先テーブルは、中継を単一の仮想ポートとして示します。

このチーム化モードでは、中間ドライバは発信トラフィックのロードバランシングとフェイルオーバーのみを制御し、受信トラフィックはスイッチのファームウェアとハードウェアで制御されます。Smart Load Balancing の場合のように、BASP 中間ドライバは IP/TCP/UDP の発信元および宛先アドレスを使用して、サーバの伝送トラフィックのロードバランスを行います。大部分のスイッチは、発信元および宛先 MAC アドレスの XOR ハッシュを搭載しています。

## 4.3.3　ソフトウェアコンポーネント

Windows の環境では、チーム化は NDIS 中間ドライバによって搭載されます。このソフトウェアコンポーネントがミニポートドライバ、NDIS レイヤー、およびプロトコルスタックで動作して、チーム化アーキテクチャを可能にします（「・中間ドライバ」（→ P.34）を参照）。ミニポートドライバは、ホスト LAN コントローラを直接制御して、送受信および割り込みの処理などの機能を有効にします。中間ドライバはミニポートドライバとプロトコルレイヤーの間に位置し、複数のミニポートドライバインスタンスを多重化して、NDIS レイヤーに対し単一アダプタのように見える仮想アダプタを作成します。NDIS は一連のライブラリ機能を提供して、ミニポートドライバまたは中間ドライバとプロトコルスタック間の通信を有効にします。プロトコルスタックは IP、IPX、および ARP を搭載します。IP アドレスなどのプロトコルアドレスは各ミニポートデバイスインスタンスに割り当てられますが、中間ドライバがインストールされている場合、プロトコルアドレスは仮想チームアダプタに割り当てられ、チームを構成する個々のミニポートデバイスには割り当てられません。

Broadcom が提供するチーム化サポートは、協調して動作しパッケージとしてサポートされる 3 つの個別のソフトウェアコンポーネントによって実現します。1 つのコンポーネントをアップグレードする場合には、他のすべてのコンポーネントもサポートされているバージョンにアップグレードする必要があります。次の表では、3 つのソフトウェアコンポーネントと、サポートしているオペレーティングシステム用の関連ファイルについて説明します。

Broadcom チーム化ソフトウェア コンポーネント

| ソフトウェアコンポーネント | Broadcom 製品の名称 | Windows ファイル名 |
|---|---|---|
| ー | 仮想バスドライバ（VBD） | bxvbdx.sys<br>bxvbda.sys (*) |
| ミニポートドライバ | Broadcom Base Driver | bxnd50x.sys<br>bxnd51x.sys<br>bxnd51a.sys (*)<br>bxnd52x.sys<br>bxnd52a.sys (*) |
| 中間ドライバ | BASP（Broadcom Advanced Server Program） | Baspxp32.sys<br>Baspw2k.sys |
| 設定ユーザーインタフェース | BACS2 | BACS2 |

*）64 ビットシステム用

## 4.3.4 ハードウェア要件

本章で説明されているさまざまなチーム化モードでは、クライアントをチーム化されたシステムに接続するためのネットワーク機器に、ある制限を設けています。各タイプのネットワークインターコネクトテクノロジーがチーム化に与える影響に関しては、これ以降のセクションで説明します。

**・リピータハブ**

リピータハブを使用すると、ネットワーク管理者はイーサネットネットワークを個々のセグメントの限界以上に拡張できます。リピータは 1 つのポートで受信した入力信号を接続されている他のすべてのポートで再生成して、単一の衝突ドメインを形成します。これは、リピータに接続されているステーションから別のステーションにイーサネットフレームを送信すると、同じ衝突ドメイン内のすべてのステーションでそのメッセージを受信するということです。2 つのステーションで同時に伝送を開始した場合、衝突が発生し、伝送中の各ステーションは任意の時間が経過した後に再度そのデータを伝送します。

リピータを使用するには、衝突ドメインに属している各ステーションが半二重モードで動作している必要があります。半二重モードは IEEE 802.3 仕様のギガビットイーサネットアダプタでサポートされていますが、ギガビットイーサネットアダプタメーカーの大部分ではサポートされていません。そのため、半二重モードはここでは考慮しません。

複数のハブにまたがるチーム化は、SLB チームに対してのみトラブルシューティング（ネットワークアナライザの接続など）の目的でサポートされています。

**・スイッチングハブ**

リピータハブとは異なり、スイッチングハブ（さらに簡単に言えば、スイッチ）を使用すると、イーサネットネットワークを複数の衝突ドメインに分けることができます。スイッチは、イーサネット MAC アドレスだけに基づいて、ホスト間でイーサネットパケットを転送する役割を果たします。スイッチに接続されている物理ネットワークアダプタは、半二重または全二重モードで動作する場合があります。

通有中継と 802.3ad リンク集約をサポートするには、スイッチでこのような機能を明確にサポートしている必要があります。スイッチでこれらのプロトコルをサポートしていない場合でも、Smart Load Balancing で使用できる場合があります。

・**ルーター**
ルーターはレイヤー 3 以上のプロトコルに基づいてネットワークトラフィックをルーティングするよう設計されていますが、スイッチング機能を持つレイヤー 2 デバイスとして動作することもよくあります。ルーターに直接接続されるポートのチーム化は、サポートされません。

## 4.3.5　チームの設定

Broadcom Advanced Control Suite 2 ユーティリティは、サポートされるオペレーティングシステム環境でチーム化の設定に使用されます。
BACS2 は、次のような 32 ビットおよび 64 ビットの Windows OS のいずれかで動作するよう設計されています。
・ Windows Server 2003
・ Windows 2000 Server
BACS2 はロードバランシングおよびフォルトトレランスのチーム化の設定と、VLAN の設定に使用されます。さらに MAC アドレス、ドライバのバージョンとステータスの情報を表示します。BACS2 には、ハードウェア診断、ケーブルテスト、およびネットワークトポロジーテストなど数多くの診断ツールも含まれています。

## 4.3.6　サポートされる機能（チームタイプ別）

次の表は、サポートされているチームタイプの機能の比較を示しています。この表を使用して、アプリケーションに最適なチームタイプを確認してください。チーム化ソフトウェアは、1 つのチームで最大 8 ポート、また 1 つのシステムで最大 4 チームをサポートします。4 つのチームにはサポートされるチーム化タイプを任意に組み合わせて使用できますが、各チームは別々のネットワークまたはサブネット上にある必要があります。

| チームタイプ | フォルトトレランス | ロードバランシング | スイッチ依存型静的中継 | スイッチ非依存型動的リンク集約（IEEE802.3ad） |
|---|---|---|---|---|
| 機能 | スタンバイを伴う SLB（*1） | SLB | 通有中継 | リンク集約 |
| チームあたりのポート数（同じブロードキャスト ドメイン） | 2 ～ 8 | 2 ～ 8 | 2 ～ 8 | 2 ～ 8 |
| チーム数 | 4 | 4 | 4 | 4 |
| アダプタフォルトトレランス | Yes | Yes | Yes | Yes |
| スイッチリンクフォルトトレランス（同じブロードキャスト ドメイン） | Yes | Yes | スイッチ依存型 | スイッチ依存型 |
| TX ロードバランシング | No | Yes | Yes | Yes |
| RX ロードバランシング | No | Yes | Yes（スイッチにより実行） | Yes（スイッチにより実行） |
| 互換スイッチが必要 | No | No | Yes | Yes |
| 接続性をチェックするためのハードビート | No | No | No | No |
| 混合メディア（異なるメディアを持つアダプタ） | Yes | Yes | Yes（スイッチ依存型） | ― |
| 混合速度（共通の速度をサポートしないが異なる速度で動作できるアダプタ） | Yes | Yes | No | No |
| 混合速度（共通の速度をサポートするが異なる速度で動作できるアダプタ） | Yes | Yes | No（同じ速度であることが必要） | Yes |

| チームタイプ | フォルトトレランス | ロードバランシング | スイッチ依存型静的中継 | スイッチ非依存型動的リンク集約（IEEE802.3ad） |
|---|---|---|---|---|
| 機能 | スタンバイを伴うSLB (*1) | SLB | 通有中継 | リンク集約 |
| ロードバランシング TCP/IP | No | Yes | Yes | Yes |
| ベンダが混在するチーム作成 | Yes (*2) | Yes (*2) | Yes (*2) | Yes (*2) |
| ロードバランシング非 IP | No | Yes（IPX アウトバウンドトラフィックのみ） | Yes | Yes |
| すべてのチームメンバに同じ MAC アドレス | No | No | Yes | Yes |
| すべてのチームメンバに同じ IP アドレス | Yes | Yes | Yes | Yes |
| IP アドレスによるロードバランシング | No | Yes | Yes | Yes |
| MAC アドレスによるロードバランシング | No | Yes（IP/IPX 以外に使用） | Yes | Yes |

*1）1 つのプライマリメンバと 1 つのスタンバイメンバがある SLB
*2）チームには少なくとも 1 つの Broadcom アダプタが必須

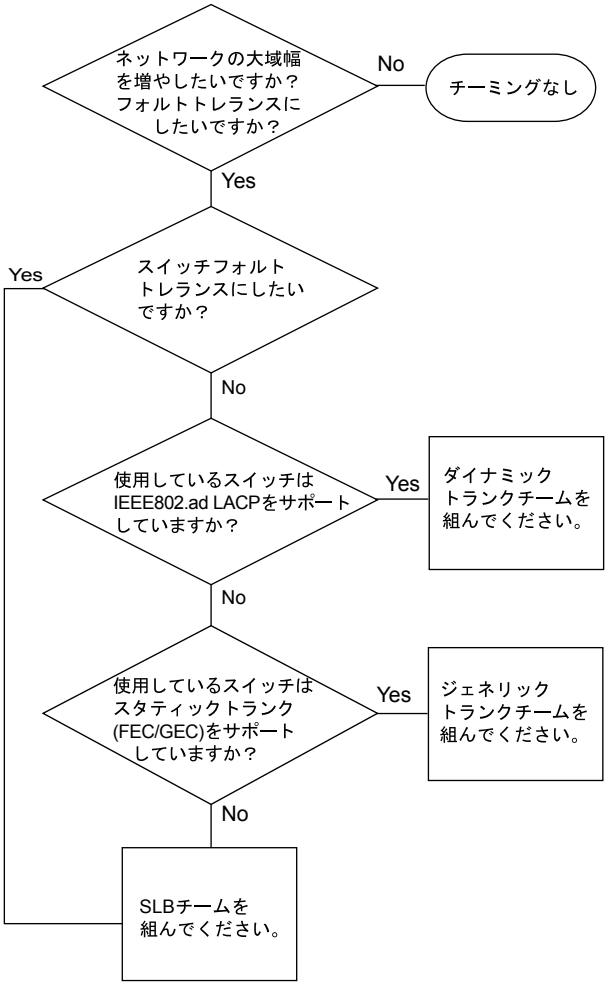
**重 要**

- ブレードサーバでは、リンク集約をサポートしていません。

## 4.3.7　チームタイプの選択

次のフローチャートでは、レイヤー 2 のチーム化を計画するときの意思決定フローを示します。チーム化を行う第 1 の理由は、ネットワーク帯域幅の増加とフォルトトレランスの向上です。チーム化により、この両方の要件を満たすためのリンク集約とフォルトトレランスが提供されます。優先するチーム化は次の順序で選択する必要があります。最初の選択として IEEE 802.3ad、第 2 の選択として通有中継、さらに、管理されていないスイッチまたは最初の 2 つのオプションをサポートしないスイッチを使用する場合は第 3 の選択として SLB チーム化。スイッチのフォルトトレランスが必要な場合は、SLB が唯一の選択肢です（次の図のチームタイプの選択のプロセスを参照）。

・チームタイプの選択のプロセス

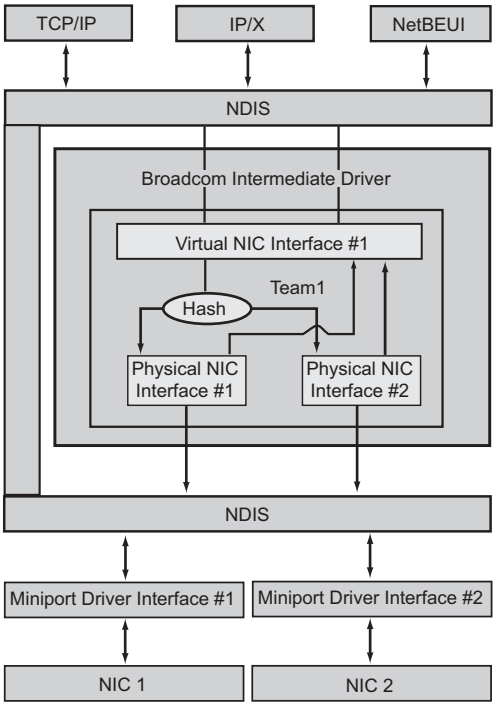


# 4.4　チーム化の仕組み

## 4.4.1　アーキテクチャ

Broadcom Advanced Server Program は、NDIS 中間ドライバとして搭載されます（「・相互接続リンクのない環境でのスイッチにまたがるチーム化」（→ P.46）を参照）。TCP/IP や IPX などのプロトコルスタックの下で動作し、仮想アダプタとして表示されます。この仮想アダプタは、チームで最初に初期化されたポートの MAC アドレスを継承します。レイヤー 3 アドレスも、仮想アダプタに対して設定する必要があります。BASP の主要機能は、チーム化することを選択されたシステムに取り付けられている物理アダプタ間で、インバウンドトラフィック（SLB の場合）とアウトバウンドトラフィック（すべてのチーム化モードの場合）のバランスをとることです。インバウンドアルゴリズムとアウトバウンドアルゴリズムは相互に独立し、直交しています。特定のセッションに対するアウトバウンドトラフィックを特定のポートに割り当て、対応するインバウンドトラフィックを別のポートに割り当てることができます。

・中間ドライバ



## 4.4.2　アウトバウンドトラフィックフロー

Broadcom 中間ドライバは、すべてのチーム化モードのアウトバウンドトラフィックフローを管理します。アウトバウンドトラフィックの場合、すべてのパケットは最初にフローに分類され、選択された物理アダプタに配分されて伝送されます。フロー分類では、既知のプロトコルフィールドに対して効率的なハッシュ計算が行われます。結果のハッシュ値を使用して、アウトバウンドフローハッシュテーブルにインデックスが作成されます。選択したアウトバウンドフローハッシュエントリには、このフローの伝送を行う選択済み物理アダプタのインデックスが含まれています。パケットのソース MAC アドレスは、選択した物理アダプタの MAC アドレスに変更されます。変更されたパケットは、選択した物理アダプタに渡されて伝送されます。

アウトバウンド TCP および UDP パケットは、レイヤー 3 およびレイヤー 4 ヘッダ情報を使用して分類されます。このスキームにより、HTTP や FTP などの well-known ポートを使用した一般的なインターネットプロトコルサービスの負荷分散が向上します。このため BASP は、パケットごとではなく TCP セッション単位でロードバランシングを実行します。

アウトバウンドフローハッシュエントリでは、分類後に統計カウンタも更新されます。ロードバランシングエンジンは、これらのカウンタを使用して、チーム化されたポート間にフローを定期的に配分します。アウトバウンドコードパスは、アウトバウンドフローハッシュテーブルへの複数の同時アクセスが許可される最善の同時性を実現するように設計されています。

TCP/IP 以外のプロトコルでは、最初の物理アダプタが常にアウトバウンドパケットに対して選択されます。例外は、インバウンドのロードバランシングを実現するために別の方法で処理される Address Resolution Protocol（ARP）です。

## 4.4.3　インバウンドトラフィックフロー（SLB のみ）

Broadcom 中間ドライバは、SLB チーム化モードのインバウンドトラフィックフローを管理します。アウトバウンドのロードバランシングとは異なり、インバウンドのロードバランシングは、ロードバランシングされたサーバと同じサブネット内にある IP アドレスにのみ適用できます。インバウンドのロードバランシングでは、Address Resolution Protocol（RFC0826）に固有の特性を利用します。各 IP ホストは独自の ARP キャッシュを使用して、IP データグラムを Ethernet フレームにカプセル化します。BASP は ARP 応答を慎重に操作し、インバウンド IP パケットを目的の物理アダプタに送信するよう各 IP ホストに指示します。このため、インバウンドのロードバランシングはインバウンドフローの統計履歴に基づいた事前計画スキームです。クライアントからサーバへの新規接続は、常にプライマリ物理アダプタ上で行われます（オペレーティングシステムプロトコルスタックによって生成された ARP 応答は常に論理 IP アドレスをプライマリ物理アダプタの MAC アドレスに関連付けるため）。
アウトバウンドの場合と同様に、インバウンドフローヘッドハッシュテーブルがあります。このテーブル内の各エントリには、単一リンクのリストがあり、各リンク（インバウンドフローエントリ）は同じサブネット内にある IP ホストを表します。

インバウンド IP データグラムが到着すると、IP データグラムのソース IP アドレスをハッシュすることによって適切なインバウンドフローヘッドエントリが検索されます。選択したエントリに格納されている 2 つの統計カウンタも更新されます。これらのカウンタは、ロードバランシングエンジンによってアウトバウンドカウンタと同じ方法で定期的に使用され、フローが物理アダプタに再割り当てされます。

インバウンドコードパスでは、インバウンドフローヘッドハッシュテーブルが同期アクセスを許可するようにも設計されています。インバウンドフローエントリのリンクリストは、ARP パケットの処理時と定期的なロードバランシング時にのみ参照されます。インバウンドフローエントリへのパケット単位の参照はありません。リンクリストがバインドされていない場合でも、ARP 以外の各パケットの処理のオーバーヘッドは常に一定です。ただし、インバウンドとアウトバウンド両方の ARP パケットの処理は、対応するリンクリスト内のリンク数に依存します。

インバウンド処理パスでは、ブロードキャストパケットが他の物理アダプタからシステムを通じてループバックすることを防ぐために、フィルタも採用されています。

## 4.4.4 プロトコルサポート

ARP および IP/TCP/UDP フローは、ロードバランシングに対応します。パケットが、ICMP や IGMP などの IP プロトコルのみの場合、特定の IP アドレスへのすべてのデータフローが同じ物理アダプタを介して送信されます。パケットが L4 プロトコルに TCP または UDP を使用している場合は、ポート番号がハッシュアルゴリズムに追加されるため、2 つの異なる L4 フローが 2 つの異なる物理アダプタを通じて同じ IP アドレスに送信されます。

たとえば、クライアントの IP アドレスが 10.0.0.1 であるとします。ハッシュには IP アドレスのみ使用されるため、すべての IGMP および ICMP トラフィックが同じ物理アダプタに送信されます。フローは次のようになります。

```
IGMP ------> PhysAdapter1 ------> 10.0.0.1
ICMP ------> PhysAdapter1 ------> 10.0.0.1
```

サーバが、同じ 10.0.0.1 アドレスに TCP および UDP フローも送信する場合、これらは IGMP および ICMP と同じ物理アダプタ上にあっても、ICMP および IGMP とはまったく異なる物理アダプタ上にあってもかまいません。ストリームは次のようになります。

```
IGMP ------> PhysAdapter1 ------> 10.0.0.1
ICMP ------> PhysAdapter1 ------> 10.0.0.1
TCP------> PhysAdapter1 ------> 10.0.0.1
UDP------> PhysAdatper1 ------> 10.0.0.1
```

または、ストリームは次のようになります。

```
IGMP ------> PhysAdapter1 ------> 10.0.0.1
ICMP ------> PhysAdapter1 ------> 10.0.0.1
TCP------> PhysAdapter1 ------> 10.0.0.1
UDP------> PhysAdatper1 ------> 10.0.0.1
```

アダプタ間の実際の割り当ては、時間の経過につれて変化する場合がありますが、ハッシュでは IP アドレスのみ使用されるため、TCP/UDP ベースでないプロトコルは同じ物理アダプタを通過します。

### 4.4.5　パフォーマンス

本製品のネットワークインタフェースカードには、特定の CPU 集中型の操作のオフローディングを行うことで CPU 利用率を軽減する多くのハードウェア機能があります（→「4.7 チーム化とその他の高度なネットワークプロパティ」(P.42)）。対照的に、BASP 中間ドライバは完全なソフトウェア機能であり、プロトコルスタックから受信した各パケットを調べて、内容に対処してから特定の物理インタフェースを通じて送信する必要があります。BASP ドライバはほぼ一定の時間で各発信パケットを処理できますが、CPU を限界まで使用している一部のアプリケーションは、チーム化されたインタフェースで動作している場合に悪影響を受けるおそれがあります。このようなアプリケーションは、ロードバランシング機能よりも中間ドライバのフェイルオーバー機能を利用する方が適切な場合があります。または、Large Send Offload（大量送信オフロード）などの特定のハードウェア機能を提供する単一の物理アダプタで、より効率的に動作する場合があります。

## 4.5　チームタイプ

### 4.4.1　スイッチ非依存型

Broadcom Smart Load Balancing チームタイプでは、2 ～ 8 の物理アダプタが単一の仮想アダプタとして動作できます。SLB チームタイプの最大の利点は、任意の IEEE 準拠スイッチで動作し、特別な設定が不要なことです。

#### ■ Smart Load Balancing（スマートロードバランス）およびフェイルオーバー

SLB は、スイッチに依存しない双方向のフォルトトレラントチーム化およびロードバランシングを提供します。スイッチに依存しないということは、スイッチ内でこの機能をサポートしている必要がなく、SLB がすべてのスイッチと互換になることを意味します。
SLB では、チーム内のすべてのアダプタに個別に MAC アドレスが与えられます。ロードバランシングアルゴリズムは、ソースおよび宛先ノードのレイヤー 3 アドレスで動作します。これにより、SLB は受信トラフィックと発信トラフィックの両方のロードバランシングを行うことが可能になります。
BASP 中間ドライバは、チーム内の物理ポートでリンクロスを継続的に監視します。いずれかのポートでリンクロスが発生した場合、トラフィックはチーム内の他のポートに自動的に転送されます。SLB チーム化モードは、異なるスイッチが同じ物理ネットワークまたはブロードキャストドメイン上にあれば、それらのスイッチ間のチーム化を許可することによりスイッチのフォルトトレランスをサポートします。

**・ネットワーク通信**

次に、SLB の主要属性を示します。

- フェイルオーバーメカニズム - リンクロス検出。
- ロードバランシングアルゴリズム - インバウンドおよびアウトバウンドトラフィックは、L4 フローに基づいて Broadcom 独自のメカニズムでバランスどりします。
- MAC アドレスを使用したアウトバウンドのロードバランシング - なし。
- IP アドレスを使用したアウトバウンドのロードバランシング - あり
- Broadcom 以外の製品を使用したチーム化サポートあり（少なくとも 1 つの Broadcom Ethernet アダプタをチームメンバとして含んでいる必要があります）。

・**アプリケーション**

SLB アルゴリズムは、コストが考慮される、または市販のスイッチング装置が使用される家庭および小規模企業環境に最も適しています。SLB チーム化は、管理されていないレイヤー 2 スイッチで動作し、サーバの冗長性とリンク集約を確保する費用対効果の高い方法となっています。Smart Load Balancing は、リンク容量が異なる物理アダプタのチーム化もサポートします。また、SLB は、チーム化したスイッチのフォルトトレランスが必要な場合にお勧めします。

・**推奨される設定**

SLB では、ハブとスイッチが同じブロードキャストドメインにある場合に、そのハブとスイッチへのチーム化されたポートの接続がサポートされます。ポートは同じサブネット上にある必要があるため、ルーターまたはレイヤー 3 スイッチへの接続はサポートしていません。

## 4.5.2　スイッチ依存型

### ■通有静的中継

アダプタリンクパートナーで占有のトランキングメカニズムをサポートするよう静的に設定されている場合、このモードでさまざまな環境がサポートできます。このモードを使用して、Lucent の Open Trunk、Cisco の Fast EtherChannel（FEC）、および Cisco の Gigabit EtherChannel（GEC）をサポートできます。通有リンク集計の場合と同様に、静的モードでは、スイッチ管理者がポートをチームに割り当てる必要があります。また、Link Aggregation Control Protocol（LACP）フレームの交換がないため、この割り当ては BASP で変更できません。

このモードでは、チーム内のすべてのアダプタが同じ MAC アドレスの受信パケットに設定されます。トランキングはレイヤー 2 アドレスで動作し、インバウンド / アウトバウンド トラフィックのロード バランシングとフェイルオーバーをサポートしています。BASP ドライバは前述のレイヤー 4 プロトコルを使用してアウトバウンド パケットのロード バランシング スキームを決定するのに対し、チームのリンク パートナーはインバウンド パケットのロード バランシング スキームを決定します。

接続されているスイッチは、この動作モードに適したトランキング スキームをサポートする必要があります。BASP とスイッチはどちらもそれぞれのポートでリンク ロスを継続的に監視します。いずれかのポートでリンク ロスが発生した場合、トラフィックはチーム内の他のポートに自動的に転送されます。

・**ネットワーク通信**

次に、通有静的中継の主要属性を示します。

- フェイルオーバー メカニズム - リンク ロス検出
- ロード バランシング アルゴリズム - アウトバウンド トラフィックは、Broadcom 独自のメカニズム ベースの L4 フローでバランス取りします。受信トラフィックは、スイッチ固有のメカニズムに従ってバランス取りします。
- MAC アドレスを使用したアウトバウンドのロード バランシング - なし
- IP アドレスを使用したアウトバウンドのロード バランシング - あり
- Broadcom 以外の製品を使用したチーム化 - サポートあり（少なくとも 1 つの Broadcom Ethernet アダプタをチーム メンバとして含んでいる必要があります）。

・**アプリケーション**

通有中継は、Cisco Fast EtherChannel、Cisco Gigabit EtherChannel、Extreme Networks Load Sharing、および Bay Networks または IEEE 802.3ad リンク集約静的モードをサポートするスイッチで動作します。ロード バランシングはレイヤー 2 アドレスに搭載されているため、IP、IPX、NetBEUI などのすべての上位プロトコルがサポートされます。したがって、これはスイッチが SLB 上での通有中継モードをサポートしている場合に推奨されるチーム化モードです。

・**推奨される設定**

静的中継では、スイッチが同じブロードキャスト ドメインにあり、通有中継をサポートしている場合に、そのスイッチへのチーム化されたポートの接続がサポートされます。ポートは同じサブネット上にある必要があるため、ルーターまたはレイヤー 3 スイッチへの接続はサポートしていません。

## ■動的中継（IEEE802.3ad リンク集約）

このモードは、Link Aggregation Control Protocol（LACP）を介した静的および動的設定によるリンク集約をサポートします。このモードでは、チーム内のすべてのアダプタが同じ MAC アドレスの受信パケットに設定されます。チーム内の最初のアダプタの MAC アドレスが使用され、別の MAC アドレスで置換できません。BASP ドライバは前述のレイヤー 4 プロトコルを使用してアウトバウンドパケットのロードバランシングスキームを決定するのに対し、チームのリンクパートナーはインバウンドパケットのロードバランシングスキームを決定します。ロードバランシングはレイヤー 2 に搭載されているため、IP、IPX、NetBEUI などのすべての上位プロトコルがサポートされます。接続されているスイッチは、この動作モードに対して 802.3ad リンク集約標準をサポートする必要があります。スイッチがアダプタへのインバウンドトラフィックを管理し、BASP がアウトバウンドトラフィックを管理します。BASP とスイッチはどちらもそれぞれのポートでリンクロスを継続的に監視します。いずれかのポートでリンクロスが発生した場合、トラフィックはチーム内の他のポートに自動的に転送されます。

・**ネットワーク通信**

次に、動的中継の主要属性を示します。

- フェイルオーバーメカニズム - リンクロス検出
- ロードバランシングアルゴリズム - アウトバウンドトラフィックは、L4 フローに基づいて Broadcom 独自のメカニズムでバランスとりを行います。受信トラフィックは、スイッチ固有のメカニズムに従ってバランスをとります。
- MAC アドレスを使用したアウトバウンドのロードバランシング - なし
- IP アドレスを使用したアウトバウンドのロードバランシング - あり
- Broadcom 以外の製品を使用したチーム化サポートあり（少なくとも 1 つの Broadcom Ethernet アダプタをチームメンバとして含んでいる必要があります）

・**アプリケーション**

動的中継は、LACP を使用した IEEE 802.3ad リンク集約の動的モードをサポートしているスイッチで動作します。インバウンドのロードバランシングはスイッチに依存します。一般に、スイッチトラフィックは L2 アドレスに基づいてロードバランシングに対応します。この場合、IP、IPX、NetBEUI などのすべてのネットワークプロトコルのロードバランシングが行われます。したがって、スイッチのフォルトトレランスが必要な場合を除き、スイッチが LACP をサポートしている場合に推奨されるチーム化モードです。SLB は、スイッチフォルトトレランスをサポートする唯一のチーム化モードです。

**・推奨される設定**

動的中継では、スイッチが同じブロードキャストドメインにあり、IEEE 802.3ad LACP 中継をサポートしている限り、そのスイッチへのチーム化されたポートの接続がサポートされます。ポートは同じサブネット上にある必要があるため、ルーターまたはレイヤー 3 スイッチへの接続はサポートしていません。

## 4.6 各チームタイプと関連する各種機能の属性

各チームタイプと関連する各種機能の属性を、次に示します。

・Smart Load Balancing™

| 機能 | 属性 |
|---|---|
| ユーザーインタフェース | BACS2 |
| チーム数 | 最大数 4 |
| チームごとのアダプタ数 | 最大数 8 |
| 動的置換 | Yes |
| 動的追加 | Yes |
| 動的削除 | Yes |
| リンク速度サポート | さまざまな速度 |
| フレームプロトコル | IP |
| インバウンドパケット管理 | BASP |
| アウトバウンドパケット管理 | BASP |
| LiveLink のサポート | Yes |
| フェイルオーバーイベント | リンクロス |
| フェイルオーバー時間 | 500 ミリ秒未満 |
| フォールバック時間 | 1.5 秒（*1）（概算） |
| MAC アドレス | 異なる |
| Broadcom 以外の製品を使用したチーム化 | Yes |

*1）Port Fast または Edge Port が有効になっていることを確認してください。

・通有中継

| 機能 | 属性 |
|---|---|
| ユーザーインタフェース | BACS2 |
| チーム数 | 最大数 4 |
| チームごとのアダプタ数 | 最大数 8 |
| 動的置換 | Yes |
| 動的追加 | Yes |
| 動的削除 | Yes |
| リンク速度サポート | さまざまな速度（*1） |
| フレームプロトコル | すべて |

| 機能 | 属性 |
|---|---|
| インバウンドパケット管理 | スイッチ |
| アウトバウンドパケット管理 | BASP |
| フェイルオーバーイベント | リンクロスのみ |
| フェイルオーバー時間 | 500 ミリ秒未満 |
| フォールバック時間 | 1.5 秒（*2）（概算） |
| MAC アドレス | すべてのアダプタに対して同一 |
| Broadcom 以外の製品を使用したチーム化 | Yes |

*1）中継接続間で正しくネゴシエートするには、リンク速度が一致していることが必要なスイッチもあります。

*2）Port Fast または Edge Port が有効になっていることを確認してください。

・動的中継

| 機能 | 属性 |
|---|---|
| ユーザーインタフェース | BACS2 |
| チーム数 | 最大数 4 |
| チームごとのアダプタ数 | 最大数 8 |
| 動的置換 | Yes |
| 動的追加 | Yes |
| 動的削除 | Yes |
| リンク速度サポート | さまざまな速度 |
| フレームプロトコル | すべて |
| インバウンドパケット管理 | スイッチ |
| アウトバウンドパケット管理 | BASP |
| フェイルオーバーイベント | リンクロスのみ |
| フェイルオーバー時間 | 500 ミリ秒未満 |
| フォールバック時間 | 1.5 秒（*1）（概算） |
| MAC アドレス | すべてのアダプタに対して同一 |
| Broadcom 以外の製品を使用したチーム化 | Yes |

*1）Port Fast または Edge Port が有効になっていることを確認してください。

### ■各チームタイプにサポートされる速度

各チームタイプにサポートされるさまざまなリンク速度を次に示します。混合速度とは、チーム化アダプタが異なるリンク速度で稼動できることを示します。

| チームタイプ | リンク速度 | トラフィックの方向 | 速度サポート |
|---|---|---|---|
| SLB | 10/100/1000 | 受信 / 発信 | 混合速度 |
| FEC | 100 | 受信 / 発信 | 同一速度 |
| GEC | 1000 | 受信 / 発信 | 同一速度 |
| IEEE 802.3ad | 10/100/1000 | 受信 / 発信 | 混合速度 |

## 4.7 チーム化とその他の高度なネットワークプロパティ

チームの作成、チームメンバの追加や削除、またはチームメンバの詳細設定の変更を行う前に、各チームメンバが同じように構成されていることを確認してください。確認する設定として、VLAN および QoS パケットタギング、ジャンボフレーム、および各種オフロードがあります。詳細なアダプタプロパティとチーム化サポートを次に示します。

| アダプタプロパティ | チーム化仮想アダプタによるサポート |
|---|---|
| Checksum Offload（チェックサムオフロード） | Yes |
| IEEE 802.1p QoS タギング | No |
| Large Send Offload（大量送信オフロード） | Yes (*1) |
| ジャンボフレーム | Yes (*2) |
| IEEE 802.1Q VLAN | Yes (*3) |
| Wake on LAN | No |
| Preboot Execution Environment（PXE） | Yes (*4) |

*1）チーム上のすべてのアダプタがこの機能をサポートしている必要があります。一部のアダプタは、ASF/IPMI も有効になっている場合にこの機能をサポートしないことがあります。

*2）チーム内のすべてのアダプタによってサポートされている必要があります。

*3）Broadcom アダプタのみ。

*4）クライアントとしてではなく PXE サーバとしてのみ。

チームは必ずしもアダプタプロパティを引き継ぐわけではなく、具体的な機能に応じて、さまざまなプロパティを備えています。たとえば、フローコントロールは、物理的なアダプタプロパティで BASP とは関係ありませんが、アダプタのミニポートドライバでフローコントロールが有効となっていれば、そのアダプタではフローコントロールが有効となります。

**POINT**

- チームがプロパティをサポートするために、チームのすべてのアダプタは、上の表に示しているプロパティをサポートする必要があります。

## ■ Checksum Offload（チェックサムオフロード）

Checksum Offload（チェックサムオフロード）はネットワークアダプタのプロパティであり、送受信トラフィックの TCP/IP/UDP チェックサムをホスト CPU ではなくアダプタハードウェアで計算できるようにします。トラフィック量が多い状況では、これにより、システムはホスト CPU がチェックサムの計算を強制される場合よりも効率的に接続を処理できます。このプロパティは本質的にハードウェアプロパティであり、ソフトウェアのみの搭載では利点を生かせません。Checksum Offload（チェックサムオフロード）をサポートするアダプタは、チェックサムをプロトコルスタックで計算する必要がないように、この機能をオペレーティングシステムに公示します。チェックサムオフロードは、現時点で IPv4 に対してのみサポートされています。

## ■ IEEE 802.1p QoS タギング

IEEE 802.1p 標準には、トラフィックの優先順位づけを可能にする 3 ビットのフィールド（最大 8 つの優先順位レベルをサポート）が含まれています。BASP 中間ドライバは、IEEE 802.1p QoS タギングをサポートしていません。

## ■ Large Send Offload（大量送信オフロード）

Large Send Offload（LSO、大量送信オフロード）は、ネットワークアダプタが提供している機能であり、TCP などの上位レベルプロトコルによって大きなデータパケットがヘッダを付加した小さな一連のパケットに分割されるのを回避します。プロトコルスタックは最大 64KB のデータパケットに対して単一のヘッダのみ生成する必要があり、アダプタハードウェアが、（最初に提供された単一ヘッダに基づいて）正しく並べられたヘッダを持つ適切なサイズの Ethernet フレームにデータバッファを分割します。

## ■ ジャンボフレーム

ジャンボフレームの使用は、元来は 1998 年に Alteon Networks, Inc. によって提案されたもので、Ethernet フレームの最大サイズを最大 9,000 バイトに増やします。正式には IEEE 802.3 Working Group によって採用されていませんが、ジャンボフレームのサポートは本製品に搭載されています。チーム内のすべての物理アダプタがジャンボフレームをサポートして、チーム内のすべてのアダプタに同じサイズが設定されていれば、BASP 中間ドライバもジャンボフレームをサポートします。

## ■ IEEE 802.1Q VLAN

1998 年に、IEEE は 802.3ac 標準を承認しました。この標準は、IEEE 802.1Q 仕様で指定されている、Ethernet ネットワーク上での Virtual Bridged Local Area Network（VLAN）タギングをサポートするフレーム形式拡張を定義しています。VLAN プロトコルでは、フレームが属する VLAN を識別するための Ethernet フレームへのタグの挿入が許可されます。現在は、4 バイトの VLAN タグが Ethernet フレームのソース MAC アドレスと長さ / タイプフールドの間に挿入されます。VLAN タグの最初の 2 バイトは IEEE 802.1Q タグタイプで構成され、次の 2 バイトにはユーザ優先順位フィールドと VLAN 識別子（VID）が含まれます。仮想 LAN（VLAN）を利用すると、ユーザは物理 LAN を論理的なサブパーツに分割できます。定義済みの VLAN は、そのトラフィックやブロードキャストがその他の VLAN から分離されるため、それぞれが独自の分離されたネットワークとして機能します。これにより各論理グループ内の帯域幅の効率が向上します。VLAN を利用すると、管理者は適切なセキュリティおよび QoS（Quality of Service、サービス品質）ポリシーを実施することもできます。BASP では、チームまたはアダプタあたり 64 個の VLAN の作成をサポートしています。63 個がタグ付きで、1 つはタグなしです。ただし、オペレーティングシステムとシステムリソースによって、実際の VLAN 数が制限されます。VLAN サポートは、IEEE 802.1Q に従って提供され、チーム化環境と単一アダプタでサポートされます。VLAN は、同種のチーム化でのみサポートされ、Broadcom 以外の製品を使用したチーム化環境ではサポートされないことに注意してください。BASP 中間ドライバは、VLAN タギングをサポートしています。1 つ以上の VLAN を中間ドライバの単一インスタンスにバインドできます。

## ■ Preboot Execution Environment：プリブート実行環境

Preboot Execution Environment（PXE）では、ネットワークを使用して、システムをオペレーティングシステムイメージから起動できます。定義上、PXE はオペレーティングシステムをロードする前に呼び出されるため、BASP 中間ドライバがチームをロードして有効にする機会はありません。したがって、オペレーティングシステムのロード時にチームに入れられる物理アダプタは、PXE クライアントとして使用できますが、チーム化機能のアダプタは PXE クライアントとしてサポートされません。チーム化されたアダプタは PXE クライアントとして使用できませんが、Dynamic Host Control Protocol（DHCP）と Trivial File Transfer Protocol（TFTP）を使用して PXE クライアントにオペレーティングシステムイメージを提供する PXE サーバではこのアダプタを使用できます。これらのプロトコルは両方とも IP に対応しており、すべてのチーム化モードによってサポートされます。

# 4.8　全般的なネットワークに関する注意事項

## 4.8.1　複数のスイッチにまたがるチーム化

SLB のチーム化は、複数のスイッチにまたがって設定できます。ただし、スイッチ同士を接続する必要があります。通有中継とリンク集約は、複数のスイッチにまたがって動作できません。その理由は、これらの搭載では、チームに含まれるすべての物理アダプタで同じイーサネット MAC アドレスを使用する必要があるためです。SLB がリンクロスを検出できるのは、チームに含まれるポート間の接続や、直接のリンクパートナーとの接続に限られるという点に注意することが重要です。SLB には、スイッチで生じる他のハードウェア障害に対応する機能がなく、他のポートのリンクロスを検出できません。

## 4.8.2　スイッチリンクのフォルトトレランス

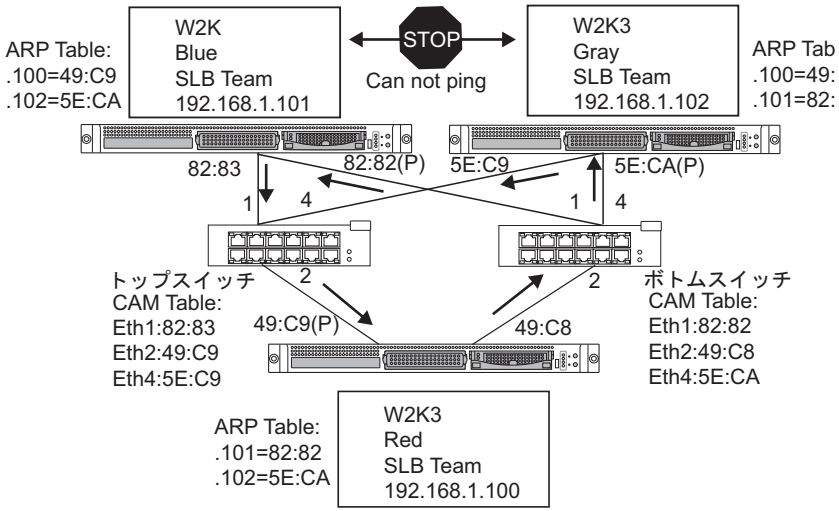
次の図では、フォルトトレランス対応のスイッチ構成でどのように SLB チームが動作するかを説明します。SLB チームにアクティブな 2 つのメンバがある構成で、ping リクエストと ping 応答メッセージのマッピングを説明します。すべてのサーバ（Blue、Gray、Red）は、継続的に ping の送受信を相互に行っています。次に、2 つのスイッチ間に相互接続ケーブルがない構成と相互接続ケーブルがある例を示します。また相互接続ケーブルがある状態でのフェイルオーバーイベントの例も示します。これらのシナリオでは、2 つのスイッチ間でのチーム化の動作を説明して、相互接続リンクの重要性を理解します。

スイッチ間に相互接続ケーブルがない構成の例では、ICMP エコー要求（点線の矢印）を送信する第 2 のチームメンバと、ICMP エコーの応答メッセージ（二重線の矢印）を受信する第 1 のチームメンバを示します。この図は、チーム化ソフトウェアの重要な特性を表しています。ロードバランシングアルゴリズムは、フレームの送受信時に、フレームのロードバランスを同期しません。言い換えると、特定の接続でのフレームは、チーム内の異なるインタフェースで送信され、受信される可能性があります。これは、Broadcom がサポートするすべてのタイプのチーム化で共通しています。したがって、同じチーム内のポートに接続するスイッチの間では、相互接続リンクを提供する必要があります。

相互接続していない構成では、Blue から Gray への ICMP 要求は、ポート 82:83 から Gray のポート 5E:CA に向けて送信されますが、Top Switch には、この要求を送信する方法がありません。なぜなら、この要求は、Gray の 5E:C9 ポートを通過できないからです。Gray が Blue に ping の送信を試行する場合にも、同じような問題が発生します。ICMP 要求は、5E:C9 から Blue の 82:82 に向けて送信されますが、この要求が受信されることはありません。Top Switch は、CAM テーブル内に 82:82 エントリを持っていません。なぜなら、2 つのスイッチの間に相互接続していないからです。ただし、ping は Red と Blue の間、Red と Gray の間では送受信されます。

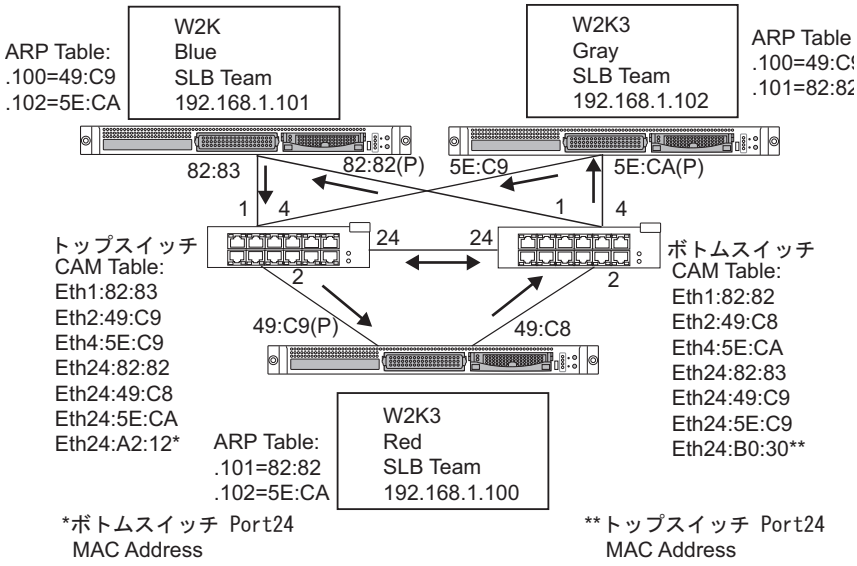
さらにフェイルオーバーイベントによって、接続が切断される場合もあります。Top Switch のポート 4 でケーブル接続の切断が生じたと仮定します。この場合、Gray は ICMP 要求を 49:C9 に送信しますが、Bottom Switch は CAM テーブル内に 49:C9 エントリを持っていないので、フレームをこれらの全ポートに配信しても、49:C9 に接続するリンクは検出できません。

・相互接続リンクのない環境でのスイッチにまたがるチーム化



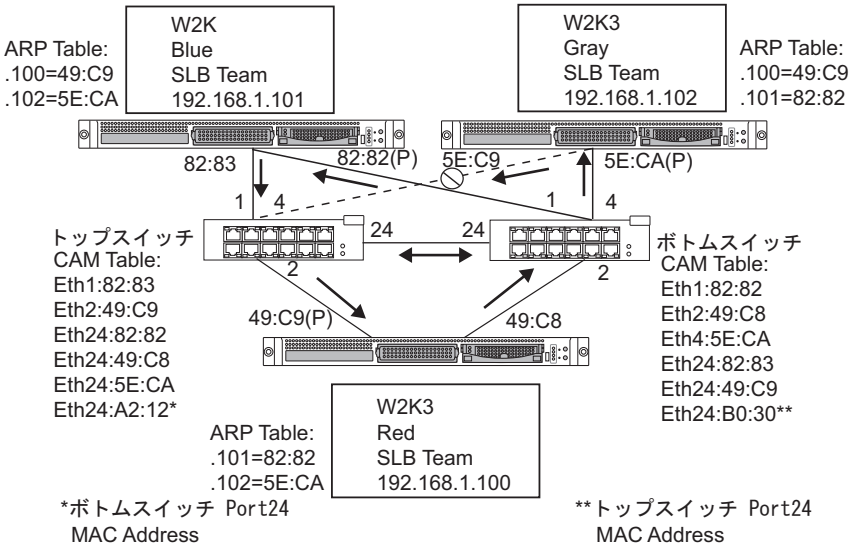

スイッチ間にリンクを設定すると、Blue と Gray の間で何の問題もなく、相互にトラフィックを送受信できます。両方のスイッチの CAM テーブルを参照して、追加されたエントリに注目してください。チームが適切に機能するには、このリンクの相互接続が重要です。したがって、2 つのスイッチを相互接続して可用性の高い接続を保証するために、リンク集約中継を使用することを強くお勧めします。

・相互接続のあるスイッチ間にまたがるチーム化



上記の図は、トップスイッチのポート 4 でケーブルが外れた場合のフェイルオーバーイベントを表しています。接続が切断されずに、すべてのステーションが相互に ping を送受信できるので、これは適切なフェイルオーバーです。

・フェイルオーバーイベント




## 4.8.3 スパニングツリーアルゴリズム

イーサネットネットワークの場合、2 つのブリッジ間またはスイッチ間では、アクティブなパスが 1 つだけ存在します。スイッチ間にアクティブなパスが複数存在していると、ネットワーク内にループが生じる可能性があります。ループが発生すると、一部のスイッチは、スイッチの両側でステーションを認識するようになります。この状況では、転送アルゴリズムが正常に機能できず、重複フレームが転送される可能性があります。スパニングツリーアルゴリズムでは、拡張ネットワーク内の全スイッチにまたがるツリーを定義して、特定の冗長データパスを強制的にスタンバイ（ブロック）状態に切り替えることで、パスの冗長性を実現します。ネットワーク内のスイッチは、パスの識別に使用するスパニングツリーパケットを定期的に送受信します。1 つのネットワークセグメントが到達不能になった場合、あるいはスパニングツリーのコストが変わった場合、スパニングツリーアルゴリズムは、スパニングツリートポロジーを再設定し、スタンバイパスをアクティブ化することでリンクを再設定します。エンドステーション側では、スパニングツリーの動作は見えません。したがって、これらのステーションでは、1 つの LAN セグメントに接続したのか、複数のセグメントで構成されたスイッチ LAN に接続したのかわかりません。

Spanning Tree Protocol（STP）は、ブリッジ間やスイッチ間での動作を目的としたレイヤー 2 プロトコルです。STP の仕様は、IEEE 802.1d で定義されています。STP の主な目的は、ネットワーク内に冗長パスがあるときにループに陥らないようにすることです。STP は、ネットワークループの検出／ディスエーブルを行い、スイッチまたはブリッジの間にバックアップリンクを提供します。このプロトコルを使用すると、デバイスは、ネットワーク内の 2 つのステーションの間で 1 つのパスのみを使用するように、ネットワークにある他の STP 準拠デバイスと相互操作を行うことが可能になります。

安定したネットワークトポロジーを確立すると、すべてのブリッジはルートブリッジから送信される hello BPDU（Bridge Protocol Data Units）を待つ状態になります。あらかじめ定義された時間（最大経過時間）が経過しても、ブリッジが hello BPDU を受信しない場合、ブリッジはルートブリッジへのリンクがダウンしたと判断します。次にこのブリッジは、他のブリッジとのネゴシエーションを開始して、ネットワークを再設定して、有効なネットワークトポロジーを再び確立します。新しいトポロジーを作成するプロセスは、最大 50 秒かかります。この間、エンドツーエンドの通信は中断されます。

エンドステーションに接続したポートに対しては、スパニングツリーは使用しないことをお勧めします。その理由は、定義上、エンドステーションは、イーサネットセグメント内でループを作成しないからです。さらにチーム化したアダプタを、スパニングツリーを有効化したポートに接続すると、接続上の不測の問題が発生する可能性があります。たとえば、チーム化したアダプタが物理アダプタの 1 つでリンクを失ったと仮定します。物理アダプタが再接続された場合（フォールバックとも呼びます）、中間ドライバはリンクが再び確立され、ポートでトラフィックの送受信が開始されたと認識します。しかし、スパニングツリープロトコルによってポートが一時的にブロックされると、トラフィックが失われることになります。

### 4.8.4　トポロジー変更通知 （TCN）

ブリッジ／スイッチは、特定のポートで受信したソース MAC アドレスから、MAC アドレスとポート番号の転送テーブルを作成します。このテーブルは、すべてのポートにフレームを配信するのではなく、特定のポートにフレームを転送するために利用します。テーブルエントリの最大の格納時間は、一般的に 5 分です。ホストでアクティビティが 5 分間ないと、エントリはテーブルから削除されます。エントリの格納時間を短くすると、効果がある場合もあります。たとえば、転送リンクがブロック状態になったときに、異なるリンクをブロック状態から転送状態に切り替えるときです。この変更には、最大 50 秒かかります。STP の再計算が完了すると、エンドステーション間の通信で、新しいパスが利用可能になります。ただし、転送テーブルには依然として古いトポロジーのエントリがあるので、5 分が経過して影響を受けるポートエントリがテーブルから削除されるまで、通信が再確立されない可能性があります。そして、トラフィックはすべてのポートに配信されて、再び取得されます。このような場合は、格納時間を短くすると効果があります。これがトポロジー変更通知（Topology Change Notice、TCN）BPDU の目的です。TCN は、影響を受けるブリッジ / スイッチからルートブリッジ / スイッチに送信されます。ブリッジ / スイッチはトポロジーの変更（リンクのダウンまたは転送状態へのポートの切り替え）を検出すると、すぐにルートポートを経由して TCN をルートブリッジに送信します。次にルートブリッジは、トポロジーの変更を通知する BPDU をネットワーク全体に配信します。この情報を受けて、すべてのブリッジは、MAC テーブルの格納時間を 15 秒に変更します。この手順により、STP の再収束のあと後すぐに、スイッチは MAC アドレスを再び取得できます。

TCN BPDU は、ポートが転送状態でからブロック状態に切り替わったとき、またはブロック状態から転送状態に切り替わったときに送信されます。TCN BPDU では、STP の再計算は開始されません。この通知は、スイッチ内の転送テーブルエントリの格納時間にのみ影響を及ぼし、ネットワークトポロジーの変更や、ループの作成は行いません。サーバまたはクライアントなどのエンドノードの場合は、電源のオフ / オン時にトポロジーの変更が開始されます。

## 4.8.5 Port Fast/Edge Port

ネットワーク上で TCN の影響（たとえば、スイッチポートで配信が増えるなど）を軽減するには、電源のオン / オフの頻度が高いエンドノードに対して、接続先になるスイッチポートで Port Fast または Edge Port を設定する必要があります。Port Fast または Edge Port は、特定のポートに適用されるコマンドであり、以下の効果があります。

・ダウンリンクからアップリンクまで、リンクに含まれる一連のポートは、待ち受け、情報の取得、転送という一連の手続きを行うのではなく、転送 STP モードに組み込まれます。STP は、依然としてこれらのポートで実行中です。
・スイッチは、ポートのアップ / ダウンのタイミングでは TCN を生成しません。

## 4.8.6 レイヤー 3 ルーティング / スイッチング

チーム化したポートを接続するスイッチは、レイヤー 3 スイッチまたはルーターである必要があります。チーム内のポートは、同じネットワークに属す必要があります。

## 4.8.7 ハブによるチーム化（トラブルシューティングの目的のみ）

10/100 ハブでは、SLB のチーム化機能を使用できますが、スイッチポートのミラーリングが使用できないときに、ネットワークアナライザに接続する場合など、トラブルシューティングの目的のみに限定することをお勧めします。

## 4.8.8 チーム化ネットワーク構成でのハブの利用

状況によって、ネットワークトポロジーでハブを使用できますが、使用する場合は、パフォーマンスに対する影響を考慮することが重要です。ネットワークハブの場合、半二重モードでは最大 100Mbps の転送速度になりますが、ギガビットまたは 100Mbps のスイッチネットワーク構成では、パフォーマンスが大幅に低下します。ハブの帯域幅は、接続されているすべてのデバイスによって共有されます。したがって、ハブに接続するデバイスが多くなると、ハブに接続したデバイス数に比例して、ハブに接続した各デバイスが使用できる帯域幅が狭くなります。

チームメンバをハブに接続することはお勧めできません。チーム化したポートに接続する場合は、スイッチのみを使用する必要があります。ただし、トラブルシューティングを目的として、SLB チームを直接的にハブに接続することができます。その他のチームタイプは、特定の障害が発生すると接続が失われる可能性があるので、ハブには使用しないでください。

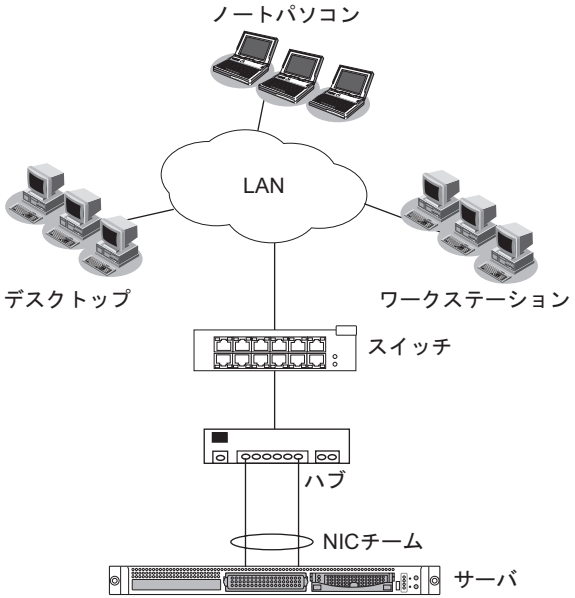
## 4.8.9 SLB チーム

SLB チームは、スイッチの設定に依存しない唯一のチームタイプです。サーバの中間ドライバは、スイッチからの支援がなくても、ロードバランシングとフォルトトレランスメカニズムを制御します。SLB にはこれらの要素があるため、チームポートをハブに直接的に接続した場合でも、フェイルオーバーとフォールバックの特性を維持できる唯一のチームタイプになっています。

### ■ 単一ハブに接続された SLB チーム

次の図のように構成された SLB チームでは、フォルトトレランスの属性が維持されます。どちらかのサーバ接続が切断された場合でも、ネットワーク機能はそのまま維持されます。クライアントをハブに直接接続することはできませんが、フォルトトレランスは維持されます。ただし、この場合、サーバのパフォーマンスは低下します。

・単一ハブに接続されたチーム




### ■ 通有中継と動的中継（FEC/GEC/IEEE802.3ad）

FEC/GEC と IEEE 802.3ad チームは、ハブの構成には接続できません。これらのチームタイプは、そのチームタイプ用に設定したスイッチに接続する必要があります。

### ■ Microsoft NLB/WLBS とのチーム化

チーム化の SLB モードは、NLB ユニキャスト環境では動作しないことが確認されています。しかし、SLB モードが NLB マルチキャスト環境で動作しない理由は知られていません。SLB チーム化アルゴリズムは、NLB ユニキャストメカニズムと相互に排他的な関係になっています。

## 4.8.10 チーム化に関する問題のトラブルシューティング

仮想アダプタのチーム化インタフェース上でプロトコルアナライザを実行すると、送信されたフレームに示される MAC アドレスが正確でない場合があります。アナライザは、BASP で構築したフレームを表示しません。フレームを転送するインタフェースの MAC アドレスでなく、チームの MAC アドレスを表示します。次の手順でチームを監視することをお勧めします。

- チームのすべてのアップリンクポートをスイッチでミラーリングします。
- チームが 2 つのスイッチにまたがる場合は、相互トランクもミラーリングします。
- すべてのミラーポートを個別にサンプリングします。
- アナライザでは、QoS と VLAN の情報をフィルタしないアダプタとドライバを使用します。

### ■チーム化の設定のヒント

ネットワーク接続またはチーム化機能のトラブルを解決するときは、次の説明が指定した設定に当てはまることを確認します。

- さまざまな速度の SLB が混在するチーム化をサポートしますが、チーム内のすべてのアダプタを同じ速度にすることをお勧めします（すべてが Gigabit Ethernet またはすべてが Fast Ethernet）。
- LiveLink が有効でない場合は、Spanning Tree Protocol を無効にするか、チームに接続するスイッチポートの初期フェーズ（Port Fast、Edge Port など）を迂回する STP モードを有効にします。
- チームを直接接続するすべてのスイッチは、同じバージョンのハードウェア、ファームウェア、ソフトウェアを使用してください。
- チーム化するには、アダプタは同じ VLAN のメンバである必要があります。複数のチームを設定する場合は、各チームが別々のネットワーク上にある必要があります。
- チームのメンバである物理アダプタには、Locally Administered Address（ローカル管理アドレス）を使用できません。
- チームを構築する前に、チームの物理メンバのそれぞれの静的 IP アドレスを削除します。
- 最大のスループットを必要とするチームには LACP または GEC/FEC を使用する必要があります。このような場合は、中間ドライバがアウトバウンドのロードバランシングのみを担当し、スイッチがインバウンドのロードバランシングを行います。
- 集約されたチーム（802.3ad/LACP および GEC/FEC）は、IEEE 802.3a、LACP、または GEC/FEC をサポートする単一のスイッチにのみ接続する必要があります。
- ハブは半二重通信しかサポートしないため、チームをハブに接続することはお勧めできません。ハブをチームに接続するのは、トラブルシューティングを目的とする場合だけにしてください。
- ベース（ミニポート）ドライバとチーム（中間）ドライバが同じリリースパッケージであることを確認します。異なる CD リリースのベースドライバとチームドライバが混在する環境でのテストを行っておらず、またサポートもしていません。
- チーム化する前に、各物理アダプタの接続をテストします。
- 実稼動環境に移行する前に、チームのフェイルオーバーとフォールバックの動作をテストします。
- 非実稼動ネットワークから実稼動ネットワークに移行する場合は、フェイルオーバーとフォールバックを再度テストすることを強くお勧めします。
- 実稼動環境に移行する前に、チームのパフォーマンスの動作をテストします。

## ■トラブルシューティングのガイドライン

システムでアダプタのチーム化を使用している場合は、次に示すネットワーク接続に関する問題のトラブルシューティングを実行してください。

- 各アダプタのリンクライトが点灯しており、すべてのケーブルが接続されていることを確認します。
- ベースドライバと中間ドライバが正しくロードされていることを確認します。
- Windows の ipconfig コマンドを使用して、IP アドレスが有効かどうかを確認します。
- チームに接続されたスイッチポートの STP が無効であることまたは Edge Port/Port Fast が有効であること、あるいは LiveLink が使用されていることを確認します。
- アダプタとスイッチのリンク速度と二重通信方式の設定が同じであることを確認します。
- 可能な場合は、チームを分割し、各アダプタへの接続を個別に調べて、問題が直接チーム化に関連することであるかどうかを確認します。
- チームに接続するすべてのスイッチポートが同じ VLAN 上に存在することを確認します。
- スイッチポートが通有中継（FEC/GEC）/802.3ad-Draft Static チームタイプ対応に正しく設定されていること、およびアダプタのチームタイプに一致していることを確認します。システムが SLB チームタイプ対応に設定されている場合は、対応するスイッチポートが通有中継（FEC/GEC）/802.3ad-Draft Static チームタイプに設定されていないことを確認します。

## ■よくある質問

| 質問 | 対応策 |
|---|---|
| どのような状況だと、トラフィックのロードバランシングは行われないのでしょうか。チームのすべてのメンバ間で均等にロードバランシングが行われないのはなぜですか。 | 大量のトラフィックが IP/TCP/UDP を使用していないか、多くのクライアントが別のネットワークに接続しています。受信のロードバランシングはトラフィック負荷に対する機能ではなく、サーバに接続するクライアントの数に対して実行される機能です。 |
| チーム内でロードバランシングが行われるネットワークプロトコルを教えてください。 | Broadcom のチーム化ソフトウェアは IP/TCP/UDP トラフィックのみをサポートします。それ以外のトラフィックはすべてプライマリアダプタに転送されます。 |
| SLB でロードバランシングが行われるプロトコルと、行われないプロトコルを教えてください。 | 送信と受信の両方向でロードバランシングが行われるのは、IP/TCP/UDP プロトコルに対してのみです。IPX に対しては送信のみロードバランシングが行われます。 |
| 100Mbps で動作するポートと 1000Mbps で動作するポートをチーム化できますか。 | 異なるリンク速度のポートの混在は、Smart Load Balancing™ のチームと 802.3ad チームでのみサポートします。 |
| ファイバーアダプタと銅線ギガビットイーサネットアダプタをチーム化できますか。 | SLB では可能です。スイッチが FEC/GEC および 802.3ad に対応する場合も可能です。 |

| 質問 | 対応策 |
| --- | --- |
| アダプタのロードバランシングと Microsoft ネットワーク負荷分散（NLB）との違いは何ですか。 | アダプタのロードバランシングはネットワークセッションレベルで行われますが、NLB はサーバアプリケーションレベルで行われます。 |
| チーム化されたアダプタをハブに接続できますか。 | チーム化されたポートはトラブルシューティングを目的とする場合にのみハブに接続できます。ただし、この方法はハブの制限によってパフォーマンスが低下するため、通常の運用ではお勧めできません。チーム化されたポートはスイッチに接続してください。 |
| チーム化されたアダプタをルーターのポートに接続できますか。 | いいえ。チーム内のポートはすべて同一のネットワーク上に存在する必要がありますが、ルーターでは定義上各ポートが個別のネットワークにあります。チーム化のすべてのモードでは、リンクパートナーがレイヤー 2 スイッチであることが必要です。 |
| Microsoft Cluster Services でチーム化を使用できますか。 | はい。チーム化は、パブリックネットワーク上でのみサポートされます。ハートビートリンクで使用するプライベートネットワークではサポートされません。 |
| PXE は仮想アダプタ（チーム）上で動作しますか。 | PXE クライアントは、オペレーティングシステムがロードされる前の環境、つまり、仮想アダプタはまだ有効になっていない状態で動作します。物理アダプタが PXE をサポートする場合は、オペレーティングシステムのロード時に仮想アダプタの要素になるかどうかにかかわらず、これを PXE クライアントとして利用できます。PXE サーバは仮想アダプタ上で動作します。 |
| ポートは最大何個までチーム化できますか。 | 最大 8 個のポートをチームに割り当てることができます。 |
| 同一のサーバ上で設定できるチームは最大何個ですか。 | 同一のサーバ上で最大 4 個のチームを設定できます。 |
| プライマリアダプタを元に戻して（フォールバック）から 30 ～ 50 秒間チームの接続が失われるのはなぜですか。 | Spanning Tree Protocol が、ポートをブロックから転送に移行させているためです。STP 遅延を考慮するには、チームに接続されたスイッチポート上で Port Fast または Edge Port を有効にするか、LiveLink を使用する必要があります。 |
| 複数のスイッチにまたがってチームを接続できますか。 | Smart Load Balancing では、システム内の個々の物理アダプタが一意の Ethernet MAC アドレスを使用するので、複数のスイッチを使用できます。リンク集約と通有中継は、すべての物理アダプタが同一の Ethernet MAC アドレスを共有するので、スイッチにまたがって動作できません。 |

| 質問 | 対応策 |
| --- | --- |
| 中間ドライバ（BASP）をアップグレードする方法を教えてください。 | 「ローカルエリア接続のプロパティ」では中間ドライバをアップグレードできません。Setup インストーラを使用してアップグレードする必要があります。 |
| NLB とチーム化を同時に設定できますか。 | はい。ただし、NLB がマルチキャストモードで動作する場合に限ります（NLB は MS Cluster Services ではサポートされません）。 |
| バックアップサーバとバックアップされるクライアントサーバの両方をチーム化する必要がありますか。 | バックアップサーバは多くのデータをロードするので、常にチーム化してリンク集約とフェイルオーバーを実現する必要があります。ただし、冗長性の十分なネットワークでは、スイッチとバックアップクライアントの両方をチーム化してフォルトトレランスとリンク集約を実現する必要があります。 |
| テープバックアップソフトウェアまたはハードウェアには、アダプタのチーム化で動作するための特別な設定が必要ですか。 | テープソフトウェアにはチーム化で動作するための特別な設定は必要ありません。テープバックアップアプリケーション側からはチーム化は見えません。 |
| 現在使用しているドライバを確認するにはどうすればよいですか。 | すべてのオペレーティングシステムにおいて、ドライバのバージョンを確認する最も確実な方法は、ドライバファイルを実際に探して、そのプロパティを確認することです。 |
| SLB は、スイッチのフォルトトレランスの設定でスイッチの障害を検出できますか。 | いいえ。SLB で検出できるのは、チーム化されたポートとその直接のリンクパートナーの間で発生するリンクロスだけです。それ以外のポートのリンク障害を検出できません。 |
| プライマリアダプタを元に戻して（フェイルオーバー後のフォールバック）から 30 ～ 50 秒間チームの接続が失われるのはなぜですか。 | フォールバックイベントの間、リンクが復元され、転送状態に移行できると判断するまで、Spanning Tree Protocol はポートにブロックを設定します。STP が原因で通信が途絶えないようにするには、チームに接続されたスイッチポート上で Port Fast または Edge Port を有効にする必要があります。 |
| Windows サーバでアダプタチームの統計をリアルタイムに監視するには、どうしたらよいでしょうか。 | BACS2 を使用して IEEE 802.3 の一般的なカウントとカスタムカウンタを監視できます。 |

# 4.9 イベントログのメッセージ

## 4.9.1 Windows システムのイベントログのメッセージ

既知のベースドライバおよび中間ドライバの本製品に関する Windows システムのイベントログのステータスメッセージを、「4.9.2 ベースドライバ（物理アダプタ / ミニポート）」（→ P.55）と「4.9.3 中間ドライバ（仮想アダプタ / チーム）」（→ P.58）に一覧を表示します。Broadcom アダプタドライバがロードされると、Windows はシステムイベントビューアにステータスコードを表示します。こうしたイベントコードには、両方のドライバがロードされたかどうかに応じて（1 つはベースドライバまたはミニポートドライバ用、もう 1 つは中間ドライバまたはチーム化ドライバ用）、最大 2 つのクラスがあります。

## 4.9.2 ベースドライバ（物理アダプタ / ミニポート）

次の表に、ベースドライバでサポートするイベントログメッセージを一覧表示し、メッセージの原因を説明します。また、推奨される対応策も示します。

・ベースドライバのイベントログメッセージ

| メッセージ番号 | メッセージ | 原因 | 対応策 |
|---|---|---|---|
| 1 | デバイスブロックにメモリを割り当てることができませんでした。システムメモリリソースの使用量を確認してください。 | ドライバはオペレーティングシステムからメモリを割り当てできません。 | 実行中のアプリケーションを閉じて空きメモリを増やします。 |
| 2 | マップレジスタを割り当てることができませんでした。 | ドライバはオペレーティングシステムからマップレジスタを割り当てできません。 | マップレジスタを割り当てる可能性のある、他のドライバをアンロードします。 |
| 3 | 構成情報にアクセスできませんでした。ネットワークドライバを再インストールしてください。 | ドライバは、アダプタ上の PCI コンフィギュレーションスペースレジスタにアクセスできません。 | アドインアダプタの場合は、アダプタをスロットに装着し直すか、アダプタを別の PCI スロットに移動するか、またはアダプタを交換します。 |
| 4 | ネットワークリンクが停止しています。ネットワークケーブルが正しく接続されているか確認してください。 | アダプタとそのリンクパートナーとの接続が失われています。 | ネットワークケーブルが接続されていることを確認し、ネットワークケーブルの種類が適切であることを調べて、リンクパートナー（スイッチまたはハブなど）が正しく機能していることを確認します。 |
| 5 | ネットワークリンクは起動しています。 | アダプタがリンクを確立しています。 | 情報提供のみを目的としたメッセージです。対応策は必要ありません。 |

| メッセージ番号 | メッセージ | 原因 | 対応策 |
|---|---|---|---|
| 6 | 10Mb 半二重リンク用にネットワークコントローラが構成されました。 | アダプタは、選択された回線速度と二重通信方式の設定に合わせて手動で構成されています。 | 情報提供のみを目的としたメッセージです。対応策は必要ありません。 |
| 7 | 10Mb 全二重リンク用にネットワークコントローラが構成されました。 | アダプタは、選択された回線速度と二重通信方式の設定に合わせて手動で構成されています。 | 情報提供のみを目的としたメッセージです。対応策は必要ありません。 |
| 8 | 100Mb 半二重リンク用にネットワークコントローラが構成されました。 | アダプタは、選択された回線速度と二重通信方式の設定に合わせて手動で構成されています。 | 情報提供のみを目的としたメッセージです。対応策は必要ありません。 |
| 9 | 100Mb 全二重リンク用にネットワークコントローラが構成されました。 | アダプタは、選択された回線速度と二重通信方式の設定に合わせて手動で構成されています。 | 情報提供のみを目的としたメッセージです。対応策は必要ありません。 |
| 10 | 1Gb 半二重リンク用にネットワークコントローラが構成されました。 | アダプタは、選択された回線速度と二重通信方式の設定に合わせて手動で構成されています。 | 情報提供のみを目的としたメッセージです。対応策は必要ありません。 |
| 11 | 1Gb 全二重リンク用にネットワークコントローラが構成されました。 | アダプタは、選択された回線速度と二重通信方式の設定に合わせて手動で構成されています。 | 情報提供のみを目的としたメッセージです。対応策は必要ありません。 |
| 12 | メディアはサポートされていません。 | オペレーティングシステムは IEEE 802.3 メディアをサポートしません。 | オペレーティングシステムを再起動して、ウィルスチェックを実行し、ディスクチェック (chkdsk) を実行して、オペレーティングシステムを再インストールします。 |
| 13 | 割り込みサービスルーチンを登録できません。 | デバイスドライバは割り込みハンドラをインストールできません。 | オペレーティングシステムを再起動し、同一の IRQ を共有する可能性のあるその他のデバイスドライバを削除します。 |
| 14 | IO 領域をマップできません。 | デバイスドライバは、メモリにマップされた I/O をアクセスドライバレジスタに割り当てできません。 | システムから他のアダプタを取り外し、インストールされた物理メモリ量を削減し、アダプタを交換します。 |
| 15 | ドライバは正常に初期化されました。 | ドライバは正常にロードされました。 | 情報提供のみを目的としたメッセージです。対応策は必要ありません。 |

| メッセージ番号 | メッセージ | 原因 | 対応策 |
|---|---|---|---|
| 16 | Ndis がミニポートドライバをリセットしています。 | NDIS レイヤーは送受信パケットの問題を検出し、ドライバをリセットして問題を解決します。 | BACS2 診断を実行し、ネットワークケーブルに問題がないことを確認します。 |
| 17 | 不明な PHY が検出されました。既定の PHY 初期化ルーチンを使用しています。 | ドライバは PHY ID を読み取れません。 | アダプタを交換します。 |
| 18 | このドライバはこのデバイスをサポートしません。最新のドライバに更新してください。 | ドライバがインストールされたアダプタを認識しません。 | このアダプタをサポートするバージョンのドライバにアップグレードします。 |
| 19 | ドライバを初期化できませんでした。 | ドライバの初期化中に特定できないエラーが発生しました。 | ドライバを再インストールするか、新しいバージョンのドライバに更新するか、BACS2 診断を実行するか、あるいはアダプタを交換します。 |

## 4.9.3　中間ドライバ（仮想アダプタ / チーム）

中間ドライバは、ベースドライバのバージョンにかかわらず、BLFM によって特定されます。次の表に、中間ドライバでサポートするイベントログメッセージを一覧表示し、メッセージの原因を説明します。また、推奨される対応策も示します。

・中間ドライバのイベントログメッセージ

| メッセージ番号 | メッセージ | 原因 | 対応策 |
|---|---|---|---|
| 1 | Unable to register with NDIS.（NDIS に登録できません。） | ドライバを NDIS インタフェースに登録できません。 | 他の NDIS ドライバをアンロードします。 |
| 2 | Unable to instantiate the management interface.（管理インタフェースをインスタンス化できません。） | ドライバはデバイスインスタンスを作成できません。 | オペレーティングシステムを再起動します。 |
| 3 | Unable to create symbolic link for the management interface.（管理インタフェース用のシンボリックリンクを作成できません。） | 別のデバイスによって競合するデバイス名が作成されています。 | Blf という名前を使用している、競合するデバイスドライバをアンロードします。 |
| 4 | Broadcom Advanced Server Program Driver has started.（Broadcom Advanced Server Program ドライバが開始しました。） | ドライバが開始しました。 | 情報提供のみを目的としたメッセージです。対応策は必要ありません。 |
| 5 | Broadcom Advanced Server Program Driver has stopped.（Broadcom Advanced Server Program ドライバが停止しました。） | ドライバはすでに停止しています。 | 情報提供のみを目的としたメッセージです。対応策は必要ありません。 |
| 6 | Could not allocate memory for internal data structures.（内部データ構造にメモリを割り当てることができませんでした。） | ドライバはオペレーティングシステムからメモリを割り当てできません。 | 実行中のアプリケーションを閉じて空きメモリを増やします。 |
| 7 | Could not bind to adapter.（アダプタにバインドできません。） | ドライバはチームの物理アダプタの 1 つを開けませんでした。 | 物理アダプタドライバをアンロードしてからリロードするか、更新された物理ドライバを取り付けるか、あるいは物理アダプタを交換します。 |
| 8 | Successfully bind to adapter.（アダプタに正常にバインドされています。） | ドライバは物理アダプタを正常に開きました。 | 情報提供のみを目的としたメッセージです。対応策は必要ありません。 |

| メッセージ番号 | メッセージ | 原因 | 対応策 |
|---|---|---|---|
| 9 | Network adapter is disconnected.（ネットワークアダプタは切断されています。） | 物理アダプタはネットワークに接続されていません（リンクが確立されていません）。 | ネットワークケーブルが接続されていることを確認し、ネットワークケーブルの種類が適切であることを調べて、リンクパートナー（スイッチまたはハブなど）が正しく機能していることを確認します。 |
| 10 | Network adapter is connected.（ネットワークアダプタは接続されています。） | 物理アダプタはネットワークに接続されています（リンクが確立されています）。 | 情報提供のみを目的としたメッセージです。対応策は必要ありません。 |
| 11 | Broadcom Advanced Program Features Driver is not designed to run on this version of Operating System.（Broadcom Advanced Program Features ドライバは、このバージョンのオペレーティングシステムでは動作しません。） | ドライバは、インストールされているオペレーティングシステムをサポートしていません。 | ドライバのリリースノートを確認し、サポートされているオペレーティングシステム上にインストールするか、ドライバを更新します。 |
| 12 | Hot-standby adapter is selected as the primary adapter for a team without a load balancing adapter.（ホットスタンバイアダプタが、ロードバランシングアダプタのないチームのプライマリアダプタとして選択されています。） | スタンバイアダプタはアクティブになっています。 | 故障した物理アダプタを交換します。 |
| 13 | Network adapter does not support Advanced Failover.（ネットワークアダプタは Advanced Failover をサポートしません。） | 物理アダプタは、Broadcom NIC Extension（NICE）をサポートしていません。 | NICE をサポートするアダプタに交換します。 |
| 14 | Network adapter is enabled via management interface.（ネットワークアダプタは、管理インタフェースを介して有効化されています。） | ドライバは、管理インタフェースを介して物理アダプタを有効化しました。 | 情報提供のみを目的としたメッセージです。対応策は必要ありません。 |

| メッセージ番号 | メッセージ | 原因 | 対応策 |
|---|---|---|---|
| 15 | Network adapter is disabled via management interface.（ネットワークアダプタは、管理インタフェースを介して無効化されています。） | ドライバは、管理インタフェースを介して物理アダプタを無効化しました。 | 情報提供のみを目的としたメッセージです。対応策は必要ありません。 |
| 16 | Network adapter is activated and is participating in network traffic.（ネットワークアダプタはアクティブ化され、ネットワークトラフィックに加わっています。） | 物理アダプタはチームに追加され、アクティブにされています。 | 情報提供のみを目的としたメッセージです。対応策は必要ありません。 |
| 17 | Network adapter is de-activated and is no longer participating in network traffic.（ネットワーク アダプタは非アクティブ化され、ネットワークトラフィックに加わっていません。） | ドライバがインストールされたアダプタを認識しません。 | 情報提供のみを目的としたメッセージです。対応策は必要ありません。 |

# 5 Broadcom Advanced Control Suite 2（BACS2）

この章では、BACS2 について説明します。

## 5.1 BACS2 の概要

BACS2 は、統合型ユーティリティであり、システムにインストールされている各ネットワークアダプタに関する情報を提供します。BACS2 では、各アダプタの詳細なテスト、診断、分析を実行できる上、プロパティ値の表示と変更や各アダプタのトラフィック情報も表示できます。

BACS2 には、次の 3 つの画面があります。
- 情報／タスク画面では、利用可能な情報を表示し、特定のタブをクリックすることで、選択したデバイスで特定のテスト、診断、分析を実行できます。
- 情報／タスク画面の左側はデバイス名画面で、個々のネットワークアダプタおよび作成された個々のチームメンバの名前が一覧表示されます。
- 3 つ目の画面にはメニューバーがあります。

Broadcom Advanced Server Program（BASP）は BACS2 内で実行され、ロードバランシング、フォルトトレランス、VLAN（Virtual Local Area Network）のチームの設定にエキスパートモードで使用します。またチームと VLAN の設定には、チーム化ウィザードを使用できます。BASP の機能は、ネットワークアダプタを少なくとも 1 つ装備しているシステムでのみ使用可能です。

**重要**

- ブレードサーバでは、リンク集約をサポートしていません。

### 5.1.1 BACS2 によって提供される情報

BACS2 は、システムのすべてのネットワークアダプタをリストし、各アダプタに関して以下の情報を提供します。

- ドライバステータス
- MAC アドレス
- リンクステータス
- IP アドレス
- メモリアドレス
- 物理アドレス
- 速度
- 二重通信方式
- スロット番号
- ドライバ名
- ドライババージョン
- ライバ更新日付
- ファームウェアバージョン
- ASIC バージョン
- バスタイプ
- バス番号
- デバイス番号
- 機能番号
- 割り込み要求
- チーム名
- チームタイプ
- VLAN 名
- VLAN ID
- プロパティ

BACS の提供する機能の詳細を、次に示します。

| 機能 | 詳細 |
|---|---|
| バイタルサイン | システム内にあるすべての LAN アダプタの情報が一目でわかります。<br>→「5.4.1 バイタルサイン」(P.67) |
| リソース | 選択したアダプタのリソース設定が表示されます。<br>→「5.4.2 リソース」(P.71) |
| ハードウェア | 選択したアダプタのハードウェア情報が表示されます。<br>→「5.4.3 ハードウェア」(P.72) |
| 詳細設定 | 選択したアダプタで利用可能なプロパティとその値が表示されます。<br>→「5.4.4 詳細設定」(P.73) |
| ネットワークテスト | リモートステーションへのネットワークの接続性を確認します。<br>→「5.4.5 ネットワークテスト」(P.76) |
| 診断 | 総合的な診断を行います。<br>→「5.4.6 診断」(P.76) |
| 統計 | トラフィック統計を確認します。<br>→「5.4.7 統計」(P.78) |
| リソースの割り当て | 割り当て済みの TOE、iSCSI、RDMA 接続と共に、未割り当てでライセンスのないリソースも含めて、円グラフが表示されます。LAN 拡張ボードのみで使用できます。<br>**POINT**<br>▸ 本設定はサポートしていません。 |
| ライセンス | TOE、iSCSI、RDMA テクノロジーのライセンス情報が表示されます。LAN 拡張ボードのみで使用できます。<br>→「5.4.8 ライセンス」(P.81) |

# 5.2 BACS2 のインストール方法

「コントロールパネル」に「Broadcom Control Suite 2」が登録されていない場合は、次の手順に従ってインストールを行ってください。

**POINT**

- BACS2 をインストールする前に、サーバブレードに LAN 拡張ボード（1Gbps）を取り付けたことを確認してください。
- インストールを開始する前に、すべてのアプリケーション、ウィンドウ、またはダイアログボックスを閉じておきます。
- TCP/IP Offload Engine（TOE）を使用するには、Scalable Networking Pack （SNP）がインストールされた Windows Server 2003 が必要です。

**重要**

- インストーラは、SNP for Windows Server 2003 がマシンにインストールされているかどうかを調べます。インストールされている場合、インストーラは、TOE の使用に必要な NDIS 5.2 ドライバをインストールします。マシンに SNP for Windows Server 2003 がインストールされていない場合、インストーラは NDIS 5.1 ドライバをインストールするので、ユーザは TOE を使用できなくなります。
- Broadcom Control Suite2 は、次の中から入手してインストールしてください。
  ・BX620 S4 サーバブレードに添付されている ServerStart CD-ROM 内の Broadcom Control Suite2
  ・弊社のインターネット情報ページ（http://primeserver.fujitsu.com/primergy/）に公開されている Broadcom Control Suite2
  なお、上記より新しい Broadcom を使用する場合は、そのドライバに添付されている取扱説明書またはヘルプファイルを参照してください。

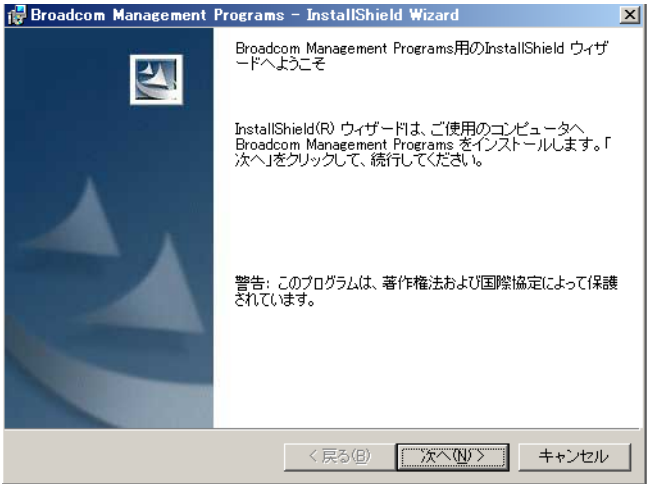
## ■ Windows Server 2003 x64 の場合

**1 ダウンロードした Broadcom Control Suite2、または BX620 S4 に添付されている ServerStart Disc1 CD-ROM 内の次の EXE を起動します。**

［CD-ROM ドライブ］：

¥PROGRAMS¥GENERAL¥Broadcom¥MgmtApps_x64¥setup.exe

インストーラが起動します。



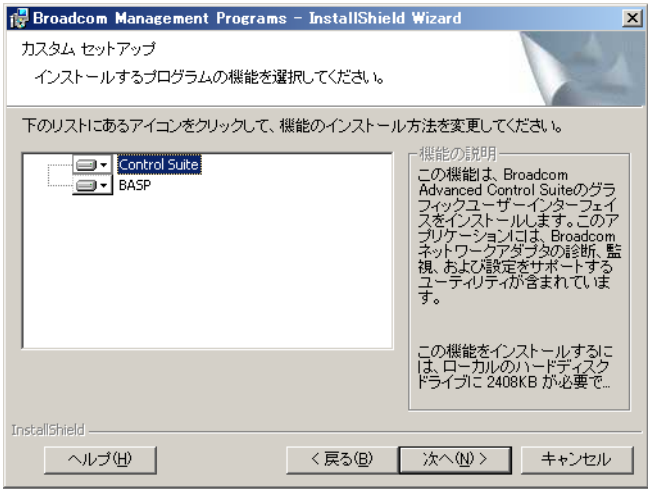

**2 ［次へ］をクリックします。**

使用許諾画面が表示されます。

Broadcom Management Programs - InstallShield Wizard
使用許諾契約
次の使用許諾契約書を注意深くお読みください。
LICENSE AGREEMENT
This is a legal agreement between you ("Licensee") and Broadcom Corporation. ("BROADCOM"). BY OPENING THE SOFTWARE PACKAGE, CLICKING ON THE "ACCEPT" BUTTON OF ANY ELECTRONIC VERSION OF THIS END USER LICENSE AGREEMENT ("AGREEMENT") OR ACCESSING OR INSTALLING THE SOFTWARE, YOU ACKNOWLEDGE THAT YOU HAVE READ THE LICENSE AGREEMENT, UNDERSTAND IT AND AGREE TO BE BOUND BY ITS TERMS AND CONDITIONS. If you do not agree to the terms
使用許諾契約の条項に同意します(A)
使用許諾契約の条項に同意しません(D)
InstallShield
< 戻る(B)
次へ(N) >
キャンセル

**3 「使用許諾契約の条項に同意します」をクリックして［次へ］をクリックします。**

カスタムセットアップ画面が表示されます。




**4 ［次へ］をクリックします。**

以降は、画面の指示に従ってインストールを行ってください。

## ■ Windows Server 2003、Windows 2000 Server の場合

**POINT**

- ServerStart を使用して OS をインストールした場合は、「BACS2」はドライバと同時にインストールされますが、手動で OS をインストールした場合は、ServerStart CD-ROM を使用した高信頼ツールの一括インストールを行うと、他の高信頼ツールと同時にインストールされます。

**1 ダウンロードした Broadcom Control Suite2、または BX620 S4 に添付されている ServerStart Disc1 CD-ROM 内の次の EXE を起動します。**

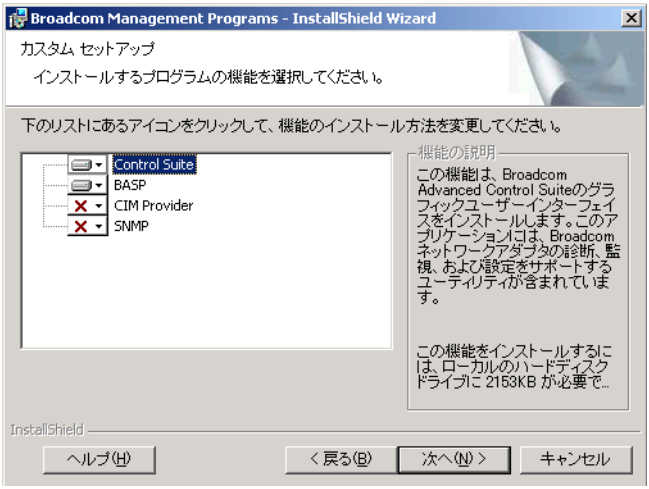
［CD-ROM ドライブ］：

¥PROGRAMS¥GENERAL¥Broadcom¥MgmtApps¥setup.exe

インストーラが起動します。

**2 画面の指示に従ってインストールを行います。**

インストールの途中で、次の画面が表示されたら、「BASP」がチェックされていることを確認して［次へ］をクリックしてください。



# 5.3 BACS2 の起動方法

BACS2 の起動方法は、「コントロールパネル」→「Broadcom Control Suite 2」の順にクリックします。
目的の情報が表示されるタブ、または必要なテスト、診断、分析、アダプタのプロパティ設定を実行するタブをクリックします。チームを作成するには、ツール」メニューの［チームの作成］をクリックします。これで、チーム化ウィザードが起動されます。

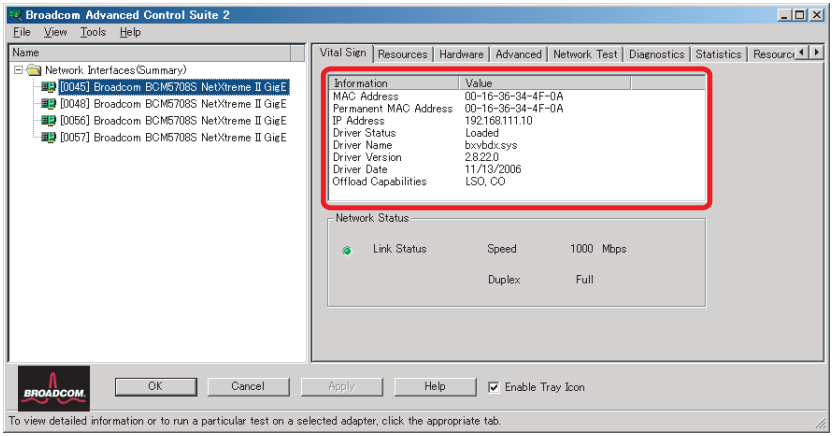
# 5.4 BACS2 の設定

## 5.4.1 バイタルサイン

「Vital Sign」タブには、LAN 拡張ボードとオンボード LAN、その他のネットワークアダプタの役立つ情報が表示されます。アダプタのリンクステータス、ネットワークの接続性などの情報が含まれます。それぞれのネットワークアダプタに関する情報を表示するには、「Name」画面にリストされているアダプタ名をクリックします。

**POINT**

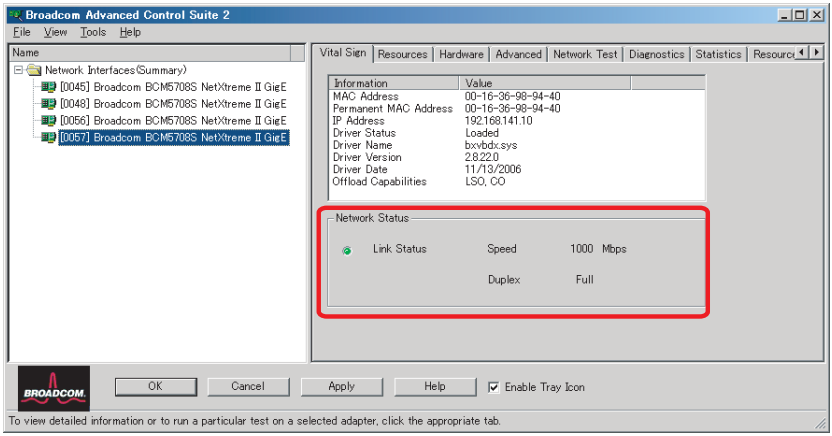
- インテル LAN カードに関する情報は、LAN 拡張ボードに比べて表示される情報量は少ないです。
- ネットワークアダプタによっては、利用できない情報もあります。



| 項目 | 説明 |
|---|---|
| MAC Address | メーカーによりアダプタに割り当てられている物理的な MAC アドレスです。物理アドレスがすべて 0 になることはありません。 |
| Permanent MAC Address | ネットワークアダプタに割り当てられている一意のハードウェアアドレスです。 |
| IP Address | アダプタに関連付けられているネットワークアドレスです。IP アドレスがすべて 0 である場合、関連付けられているドライバがインターネットプロトコル（IP）にバインドされていないことを示しています。 |
| Driver Status | アダプタドライバのステータスです。 |
| Loaded | 通常動作モードです。アダプタドライバはロードされ、動作しています。 |
| Not Loaded | アダプタに関連付けられているドライバは、Windows によってロードされていません。 |
| Information Not Available | アダプタに関連付けられているドライバから取得可能な値はありません。 |
| Driver Name/ Version/Date | アダプタドライバのファイル名です。 |
| LiveLink IP Address | LiveLink 対応アダプタのネットワークアドレスです。 |
| Offload Capabilities | アダプタによってサポートされるオフロード機能です。 |
| LSO | Large Send Offload（大量送信オフロード）は、TCP などの上位レベルプロトコルによって大きなデータパケットがヘッダを付加した小さな一連のパケットに分割されるのを回避します。 |
| CO | Checksum Offload（チェックサム オフロード）は、送受信トラフィックの TCP/IP/UDP チェックサムをホスト CPU ではなくアダプタハードウェアで計算できるようにします。 |
| BASP State | BASP アプリケーションのステータスに関する情報です。この情報は、チームがある場合にのみ表示されます（→「1.3.3 チームの機能」(P.10)）。 |

## ■ネットワークステータス

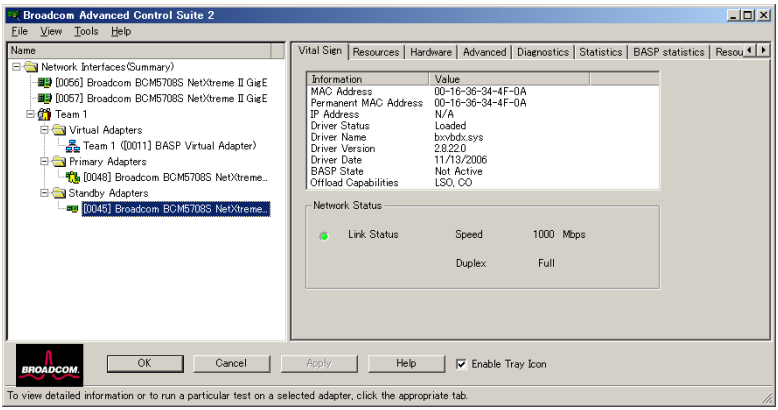
「Network Status」画面では、次のネットワークステータス情報を確認できます。



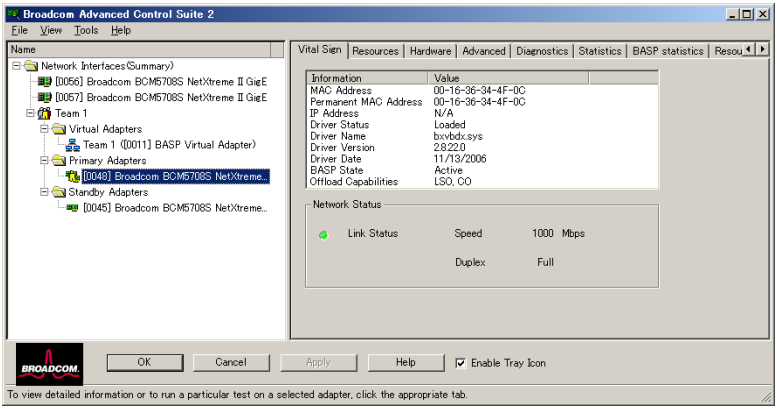

| 項目 | 説明 |
|---|---|
| Link Status | リンクが確立されると、インジケータは緑になります。インジケータが赤い場合、リンクは確立されていません。 |
| Speed | アダプタのリンク速度です。 |
| Duplex | アダプタが半二重、全二重のどちらで動作しているかを示します。 |

## ■チームのステータス

チームのステータスは、チームおよびチームメンバを示すアイコンによって示されます。アダプタアイコンにアダプタのみが表示されている場合、アダプタはネットワークに接続されていますが、チームに正しく参加していません。これは、非アクティブ BASP ステータスに該当します。この条件は、チームのスタンバイメンバであるアダプタには適用されません。非アクティブであっても、スタンバイアダプタは適切に機能している場合があります。



アダプタアイコンに実行中の黄色の人の姿が表示されている場合、アダプタは接続され、チームに正しく参加しています。これは、アクティブ BASP ステータスに該当します。



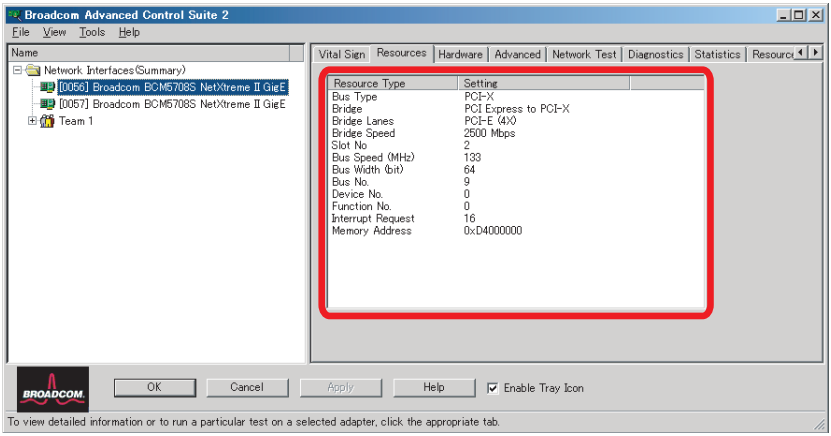

アダプタアイコンに赤い文字の X が表示されている場合、アダプタはネットワークに接続されていません。

## 5.4.2　リソース

「Resources」タブでは、次の情報を確認できます。

**POINT**

- ネットワークアダプタによっては、利用できない情報もあります。



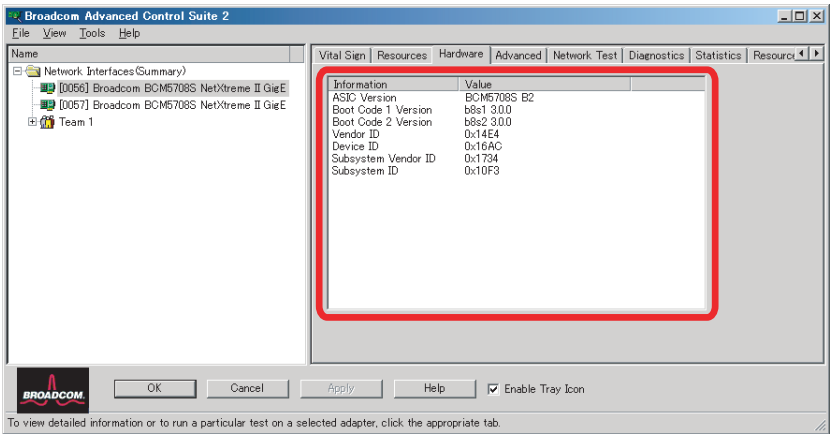

| 項目 | 説明 |
|---|---|
| Bus Type | アダプタが使用する入力 / 出力（I/O）インターコネクトのタイプです。 |
| Bridge | ブリッジタイプです。ここでは、PCI-E to PCI-X ブリッジです。 |
| Bridge Lanes | ブリッジに接続されている PCI-E レーンの数です。 |
| Bridge Speed | PCI-E バスのクロックスピードです。 |
| Slot No | アダプタが使用するシステムボード上のスロット番号です。 |
| Bus Speed（MHz） | アダプタが使用するバスクロックシグナルの周波数です。 |
| Bus Width（bit） | バスがアダプタとの間で一度に転送できるビット数です。 |
| Bus No | アダプタをインストールしたバスの番号を示します。 |
| Device No | オペレーティングシステムによってアダプタに割り当てられた番号です。 |
| Function No | アダプタのポート番号です。シングルポートのアダプタの場合、機能番号は 0 になります。2 ポートのアダプタの場合、最初のポートの機能番号は 0 に、2 つ目のポートの機能番号は 1 になります。 |
| Interrupt Request | アダプタに関連付けられている割り込み線番号です。有効値の範囲は 2 ～ 25 です。 |
| Memory Address | アダプタに割り当てられている、メモリにマップされたアドレスです。この値が 0 になることはありません。 |

## 5.4.3　ハードウェア

「Hardware」タブでは、次の情報を確認できます。

**POINT**

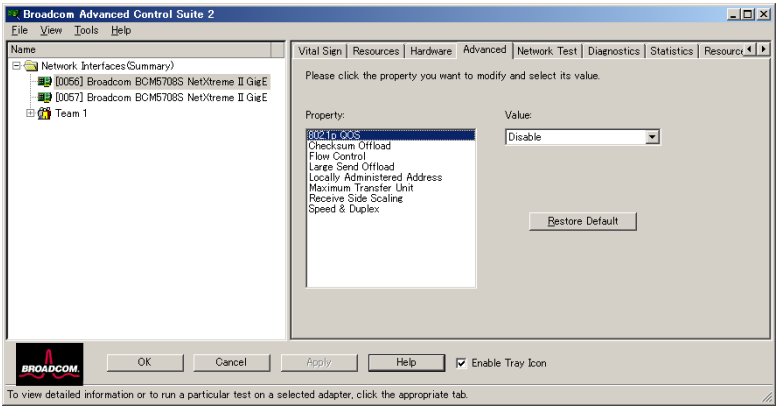
- ネットワークアダプタによっては、利用できない情報もあります。




| 項目 | 説明 |
|---|---|
| ASIC Version | Broadcom アダプタのチップバージョンです（他社製アダプタの場合には、この情報は表示されません）。 |
| Boot Code 1 Version | ブートコード 1 のバージョンです。 |
| Boot Code 2 Version | ブートコード 2 のバージョンです。 |
| Vendor ID | ベンダ ID です。 |
| Device ID | アダプタ ID です。 |
| Subsystem Vendor ID | サブシステムベンダ ID です。 |
| Subsystem ID | サブシステム ID です。 |

## 5.4.4　詳細設定

「Advanced」タブでは、次の情報を確認できます。




「Advanced」タブでは、選択したアダプタの利用可能なプロパティの値を表示および変更できます。利用可能なプロパティとその設定について以下で説明します。プロパティの値を表示するには、「Property」リスト内のプロパティ名をクリックします。プロパティの値は、「Value」ボックスに表示されます。値を変更するには、必要に応じて「Value」リスト内の項目をクリックするか新しい値を入力します（選択オプションはプロパティごとに異なります）。

**POINT**

- **プロパティの値を変更するには、管理者特権が必要です。**
- **ご使用のアダプタの利用可能なプロパティのリストは異なる場合があります。**
- **ネットワークアダプタによっては、利用できないプロパティもあります。**

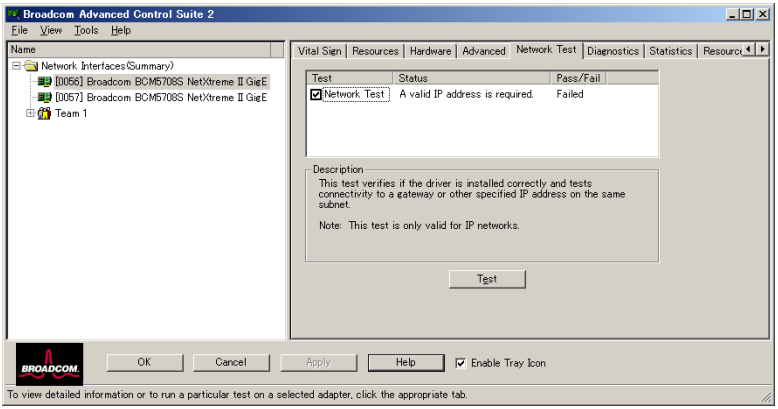
| 項目 | 説明 |
|---|---|
| 802.1p QOS | 802.1p QOS のプロパティは、QOS（Quality of Service、サービス品質）を有効にします。これは IEEE（Institute of Electrical and Electronics Engineering、米電気電子学会）の仕様であり、必要な品質レベル、信頼性、待ち時間を実現するために、トラフィックのタイプに応じて、さまざまなタイプのネットワークトラフィックを異なる方式で制御するものです。このプロパティは、デフォルトで無効に設定されています。ネットワーク環境が QoS をサポートしている場合を除いて、QoS は有効にしないでください。有効にすると、問題が発生する可能性があります。 |

| 項目 | 説明 |
| --- | --- |
| Checksum Offload（チェックサムオフロード） | チェックサム機能は通常、プロトコルスタックによってコンピュータ計算されます。Checksum Offload（チェックサムオフロード）のプロパティ値のいずれか（None（なし）以外）を選択すると、ネットワークアダプタによるチェックサムの計算が可能になります。<br>・ Rx TCP/IP Checksum（Rx TCP/IP チェックサム）<br>TCP/IP/UDP の受信パケットの Checksum Offload（チェックサムオフロード）を有効にします。<br>・ Tx TCP/IP Checksum（Tx TCP/IP チェックサム）<br>TCP/IP/UDP の転送パケットの Checksum Offload（チェックサムオフロード）を有効にします。<br>・ Tx/Rx TCP/IP Checksum（Tx/Rx TCP/IP チェックサム）（デフォルト）<br>TCP/IP/UDP の受信 / 転送パケットの Checksum Offload（チェックサムオフロード）を有効にします。<br>・ None（なし）<br>Checksum Offload（チェックサムオフロード）を無効にします。 |
| Flow Control（フローコントロール） | Flow Control（フローコントロール）のプロパティは、PAUSE フレームの受信・転送の有効／無効を切り替えます。PAUSE フレームは、ネットワークアダプタとスイッチで速度をコントロールできるようにします。PAUSE フレームを受信している側は、一時的に受信を停止します。<br>・ Auto（自動）（デフォルト）<br>PAUSE フレームの受信と転送が最適化されます。<br>・ Disable（無効）<br>PAUSE フレームの受信と転送を無効にします。<br>・ Rx PAUSE<br>PAUSE フレームの受信を有効にします。<br>・ Rx/Tx PAUSE<br>PAUSE フレームの受信と転送を有効にします。<br>・ Tx PAUSE<br>PAUSE フレーム転送を有効にします。 |
| Large Send Offload（大量送信オフロード） | TCP の区分化は通常、プロトコルスタックによって実行されます。Large Send Offload（大量送信オフロード）のプロパティを有効にすると、ネットワークアダプタによる TCP の区分化が可能になります。<br>・ Disable（無効）<br>Large Send Offload（大量送信オフロード）を無効にします。<br>・ Enable（有効）（デフォルト）<br>Large Send Offload（大量送信オフロード）を有効にします。 |

| 項目 | 説明 |
| --- | --- |
| Locally Administered Address（ローカル管理アドレス） | Locally Administered Address（ローカル管理アドレス）は、ユーザ定義の MAC アドレスで、ネットワークアダプタにもともと割り当てられている MAC アドレスの代わりに使用されます。ネットワーク内にあるアダプタには、それぞれ一意の MAC アドレスが必要です。このローカル管理アドレスは、12 桁の 16 進数で構成されています。<br>・Value（値）<br>アダプタに一意のノードアドレスを割り当てます。<br>・Not Present（存在しません）（デフォルト）<br>工場出荷時に割り当てられたノードアドレスをアダプタに使用します。<br>ローカル管理アドレスについて、該当する割り当て範囲と例外は次のとおりです。<br>・範囲は 00:00:00:00:00:01 ～ FF:FF:FF:FF:FF:FD です。<br>・マルチキャストアドレスは使用しないでください（もっとも有意度の低いバイト＝ 1）。<br>・すべてを 0 としたり、F としたりすることはできません。 |
| Maximum Transfer Unit（最大転送単位） | Maximum Transfer Unit（最大転送単位）のプロパティを使用すると、1514 バイトより大きく、長さが 9000 バイト以下の Ethernet フレームをネットワークアダプタで受信したり、転送したりすることができるようになります。このプロパティには、ジャンボフレームを処理できるスイッチが必要となります。<br>フレームサイズはデフォルトでは 1500 バイトに設定されています。受信フレームのサイズを大きくするときは、バイト量を 500 バイトずつ増やしてください。 |
| Speed & Duplex（速度と二重通信方式） | Speed & Duplex（速度と二重通信方式）のプロパティでは、ネットワークへの接続速度や通信方式を設定します。全二重通信方式モードにすると、アダプタでのネットワークデータ受信・転送が同時にできるようになります。<br>・10 Mb Full（10Mb 全二重）<br>速度を 10Mbit/ 秒に、通信方式を全二重に設定します。<br>・10 Mb Half（10Mb 半二重）<br>速度を 10Mbit/ 秒に、通信方式を半二重に設定します。<br>・100 Mb Full（100Mb 全二重）<br>速度を 100Mbit/ 秒に、通信方式を全二重に設定します。<br>・100 Mb Half（100Mb 半二重）<br>速度を 100Mbit/ 秒に、通信方式を半二重に設定します。<br>・Auto（自動）<br>速度と通信方式をネットワークに最適な接続に設定します。 |

## 5.4.5　ネットワークテスト

「Network Test」タブでは、IP ネットワークの接続性を検証できます。このテストは、ドライバが正しくインストールされているかどうかを確認し、また、同一サブネット上で他に指定されている IP アドレスやゲートウェイへの接続性を検証します。ネットワークテストでは TCP/IP が使用されます。ネットワークテストでは ICMP パケットをリモートシステムに送信し、応答を待ちます。ゲートウェイが設定されている場合は、リモートシステムにパケットが自動的に送信されます。ゲートウェイが設定されていない場合、またはゲートウェイに到達できない場合は、宛先の IP アドレスを指定するよう要求されます。

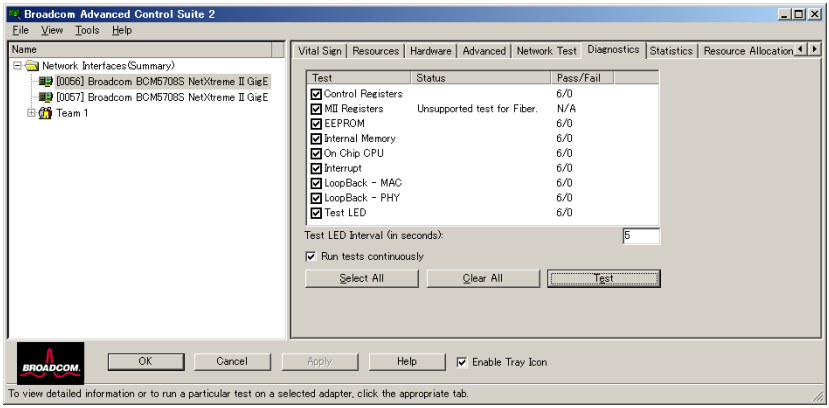



## 5.4.6　診断

「Diagnostics」タブでは、ネットワークアダプタの物理コンポーネントを対象にした診断テストを実行することができます。テストは、継続的に実行されます。「パス / 失敗」コラムのパス数と失敗数は、テストが実行されるたびに増加します。たとえば、テストが 4 回実行され、失敗がなかった場合、「パス / 失敗」コラムの値は 4/0 です。パスが 3 回で失敗が 1 回あった場合、「パス / 失敗」コラムの値は 3/1 です。

**POINT**

- 診断を実行するには、Windows の管理者特権が必要です。
- テストの実行中に、ネットワーク接続が一時的に失われます。



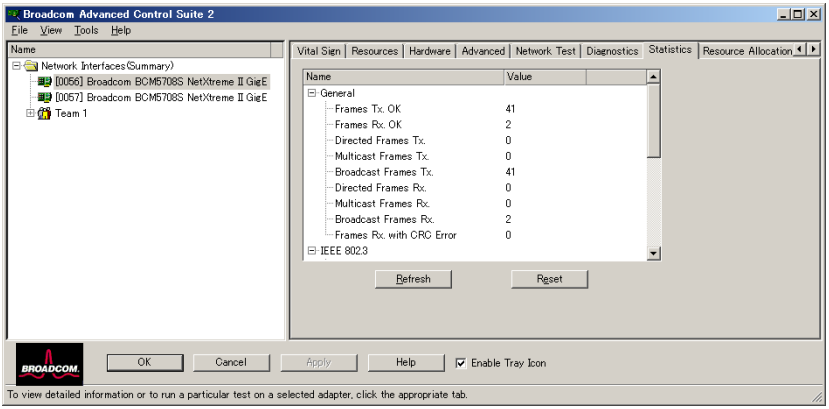

| 項目 | 説明 |
|---|---|
| Control Registers | このテストはネットワークアダプタレジスタの読み書き能力を検証するもので、レジスタに対してさまざまな値を書き込み、その結果を検証します。アダプタドライバはネットワークコントローラレジスタを使用し、データ送受信などのネットワーク機能を実行します。テストに失敗した場合は、アダプタが正しく動作していない可能性があります。 |
| MII Registers | このテストは、物理層（PHY）のレジスタの読み書き能力を検証します。物理層は、ワイヤ上の電気信号を制御し、1,000Mbit/ 秒というネットワーク速度を設定するために利用されています。 |
| EEPROM | このテストは、EEPROM（Electrically Erasable Programmable Read-only Memory）の一部を読み出し、チェックサムをコンピュータ計算して EEPROM のコンテンツを検証します。コンピュータ計算したチェックサムが EEPROM 内に保存されているチェックサムと異なる場合、テストは失敗となります。EEPROM イメージのアップグレードでは、このテストのコードを変更する必要はありません。 |
| Internal Memory | このテストでは、アダプタの内部メモリが正しく機能しているかを確認します。テスト時は、パターン化された値をメモリに書き込み、その結果を読み出します。誤った値が読み戻されると、テストは失敗となります。内部メモリが正しく機能していないと、アダプタは機能しません。 |
| On-Chip CPU | このテストでは、アダプタ内の内部 CPU の動作を検証します。 |
| Interrupt | このテストでは、NDIS（Network Device Driver Interface Specification）ドライバがアダプタからの割り込みを受信できるかどうかを検証します。 |
| Loopback MAC and Loopback PHY | このテストでは、NDIS ドライバとアダプタ間でパケットの送受信ができるかどうかを検証します。 |
| Test LED | このテストでは、特定のアダプタを識別するために、すべてのポート LED を 5 回点滅させます。 |

## 5.4.7　統計

「Statistics」タブでは、トラフィック統計を確認することができます。この情報は、ネットワークアダプタが Broadcom 製でなくても確認できますが、統計情報と統計の対象は、Broadcom アダプタの方が広範囲にわたります。

**POINT**

- ネットワークアダプタによっては、利用できない統計もあります。




### ■ General

| 項目 | 説明 |
|---|---|
| Frames Tx. OK | 無事転送されたフレーム数のカウントです。このカウンタは、転送ステータスが Transmit OK（転送 OK）とレポートされるとインクリメントします。 |
| Frames Rx. OK | 無事受信されたフレーム数のカウントです。これには、長すぎるフレーム、フレーム チェックシーケンス（FCS）、長さ・アラインメントエラー、内部 MAC サブレイヤーエラーによるフレーム損失などが発生したフレームは含まれません。このカウンタは、受信ステータスが Receive OK（受信 OK）とレポートされるとインクリメントします。 |
| Directed Frames Tx | 無事転送された伝送データフレーム数のカウントです。 |
| Multicast Frames Tx. | 同報通信アドレス以外のグループ宛先アドレスに無事転送されたフレーム数のカウントです（ステータス値は Transmit OK）。 |
| Broadcast Frames Tx. | 同報通信アドレスに無事転送されたフレーム数のカウントです（転送ステータスは Transmit OK）。マルチキャストアドレスへ転送されたフレームは同報通信フレームにはならないため、除外されます。 |
| Directed Frames Rx. | 無事受信された伝送データフレーム数のカウントです。 |

| 項目 | 説明 |
|---|---|
| Multicast Frames Rx. | 無事受信され、アクティブの非同報通信グループアドレスに伝送されたフレーム数のカウントです。これには、長すぎるフレーム、FCS、長さ・アラインメントエラー、内部 MAC サブレイヤーエラーによるフレーム損失などが発生したフレームは含まれません。このカウンタは Receive OK ステータスが示されるとインクリメントします。 |
| Broadcast Frames Rx. | 無事受信され、同報通信グループアドレスに伝送されたフレーム数のカウントです。このカウントには、長すぎるフレーム、FCS、長さ・アラインメントエラー、内部 MAC サブレイヤーエラーによるフレーム損失などが発生したフレームは含まれません。このカウンタは Receive OK ステータスが示されるとインクリメントします。 |
| Frames Rx. with CRC Error | CRC エラーで受信されたフレーム数です。 |

## ■ IEEE 802.3

| 項目 | 説明 |
|---|---|
| Frames Rx. with Aligment Error | 長さが 8 ビットバイトで積分できない数値であるために FCS チェックを通過できなかったフレーム数のカウントです。このカウンタは、受信ステータスが Alignment Error（アラインメントエラー）とレポートされるとインクリメントします。 |
| Frames Tx. with One Collision | 衝突が 1 回あったものの、無事転送が済んだフレーム数のカウントです。このカウンタは、転送結果が Transmit OK（転送 OK）とレポートされ、試行値が 2 になるとインクリメントします。 |
| Frames Tx. with more than One Collision | 衝突が複数回あったものの、無事転送が済んだフレーム数のカウントです。このカウンタは、転送ステータスが Transmit OK（転送 OK）とレポートされ、試行変数の値が 2 より大きく、試行限界値以下のときインクリメントします。 |
| Frames Tx. after Deferral | 媒体がビジーであったために、最初の試行で転送が遅延されたフレーム数のカウントです。衝突に関連したフレームはカウントされません。 |

## ■ Custom

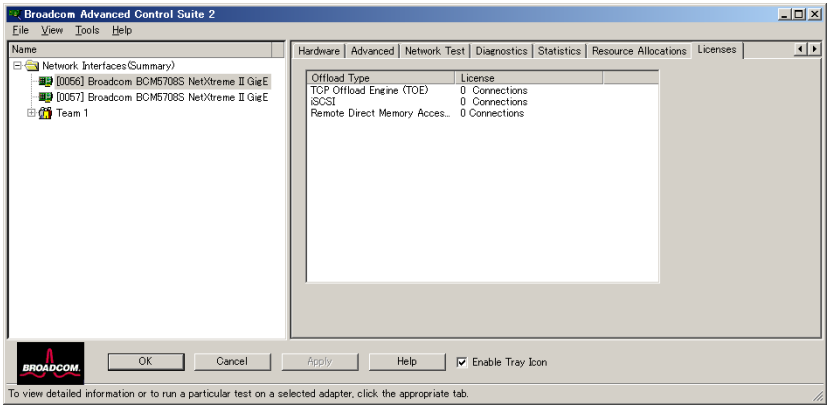
| 項目 | 説明 |
|---|---|
| Out of Recv. Buffer | アダプタで受信バッファ記述子が足りなくなった回数です。 |
| Frames size less than 64 bytes with bad FCS | FCS が劣悪なためにフレームサイズが 64 バイト以下になったフレーム数です。 |
| MAC Rx. w/Pause Command and Length=0 | ポーズコマンドで指定され、長さが 0 である MAC コントロールフレームがあることを示します。 |
| MAC Rx. w/Pause Command and Length > 0 | ポーズコマンドで指定され、長さが 0 よりも大きい MAC コントロールフレームがあることを示します。 |
| MAC Rx. w/no pause Command | ポーズコマンドで指定されていない MAC コントロールフレームがあることを示します。 |
| MAC Sent Xon | X-on での MAC 転送がオンになっています。 |
| MAC Sent Xoff | X-on での MAC 転送がオフになっています。 |
| Large Send Offload Transmit Requests. | アダプタが TCP の区分化を実行するパケットの転送を要求された回数です。 |

## 5.4.8　ライセンス

「Licenses」タブでは、TOE、iSCSI、RDMA オフロードテクノロジーで利用できる接続数を表示できます。

**POINT**

- 「Licenses」タブが利用できるのは、LAN 拡張ボードのみです。
- アダプタによっては、利用できないオフロードテクノロジーもあります。



# 5.5　チームの設定

チーム化機能を使用すると、ネットワークアダプタをグループ化し、チームとして機能します。チーム化は、バーチャル LAN（1 つのアダプタとして機能する複数のアダプタのグループ）を作成する方法の 1 つです。この方法の利点は、ロードバランシングとフェイルオーバーが可能になることです。チーム化は Broadcom Advanced Server Program（BASP）ソフトウェアを使用して実行します。チーム化ソフトウェアの技術および搭載の留意事項に関する総合的な説明については、「4 Broadcom Gigabit Ethernet のチーム化サービス」（→ P.21）を参照してください。

チーム化は、次の方法のいずれかで実行できます。

・Broadcom チーム化ウィザードを使用する
→「5.5.2 チーム化ウィザードを使用してチームを作成および変更する」（P.83）

・エキスパートモードを使用する
→「5.5.3 エキスパートモードを使用する」（P.91）

**POINT**

- チームの設定時に LiveLink™ を有効にしない場合は、スイッチでスパニングツリープロトコル（STP）を無効にしてください。これにより、フェイルオーバー時のスパニングツリーループ決定によるダウンタイムが最低限に抑えられます。LiveLink は、このような問題を可能な限り回避します。
- BASP は、Microsoft Network Load Balancing（NLB）をサポートしていません。
- Large Send Offload（LSO、大量送信オフロード）および Checksum Offload（チェックサムオフロード）のプロパティは、LSO、Checksum Offload がチームのすべてのメンバでサポートおよび設定されている場合にのみ、チームに対して自動的に有効化されます。
- チームを作成、変更するには、管理者特権が必要です。
- チームメンバがそれぞれ異なる速度で接続している環境でのロードバランスアルゴリズムでは、ギガビットイーサネットリンクで接続しているメンバのほうが、しきい値に達するまで低速リンク（100 Mbps または 10Mbps）で接続しているメンバよりも有利です。これは通常の動作です。

チームの詳細については、「1.3.3 チームの機能」（→ P.10）を参照してください。

**重要**

- ブレードサーバでは、リンク集約をサポートしていません。

## 5.5.1 Broadcom チーム化ウィザードを使用する

Broadcom チーム化ウィザードを使用して、チームの作成、既存のチーム（チームがすでに作成されている場合）の設定、または VLAN の作成を行うことができます。

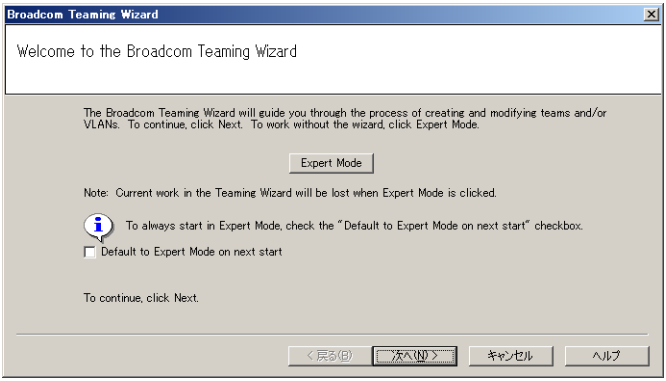
## 5.5.2 チーム化ウィザードを使用してチームを作成および変更する

**1 BACS2 の「Tools」→「Create a Team」の順にクリックします。**

**POINT**

- 常にエキスパートモードを使用してチームを作成する場合は、「Default to Expert Mode on next Start」をオンにします。ウィザードを使用しない場合は、「Expert Mode」をクリックし、［Next］をクリックします。「5.5.3 エキスパートモードを使用する」（→ P.91）を参照してください。

**2 ウィザードを使用して続行する場合は、［次へ］をクリックします。**




**3 チーム名を入力し、［次へ］をクリックします。**

・設定を確認または変更する場合は、［戻る］をクリックしてください。
・設定を破棄してウィザードを終了するには、［キャンセル］をクリックしてください。

**POINT**

- チーム名は最大 39 文字で、スペースで開始することはできず、次の文字は使用できません。
  ・& \ / : * ? < > |

J

**4 作成するチームタイプを選択し、［次へ］をクリックします。**

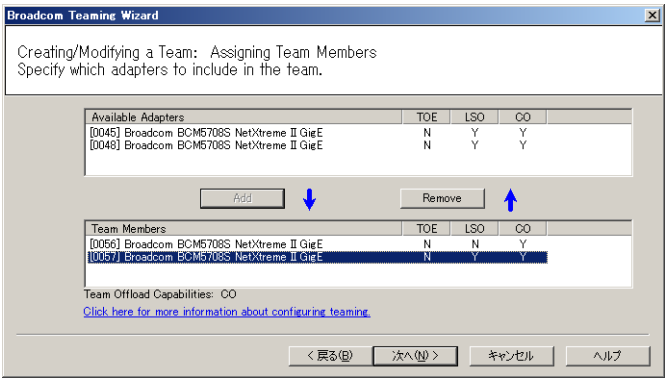
チームタイプが SLB タイプのチームの場合、［Next］をクリックします。チームタイプが SLB タイプのチームではない場合、ダイアログボックスが表示されます。チームメンバに接続されたネットワークスイッチが、チームタイプに対して適切に設定されていることを確認し、［OK］をクリックして続行してください。

**5 「Available Adapters」リストで、チームに追加するアダプタをクリックし、［Add］をクリックします。チームメンバを「Team Members/ チーム メンバ」リストから削除する場合は、アダプタをクリックし、［Remove］をクリックして、［次へ］をクリックします。**

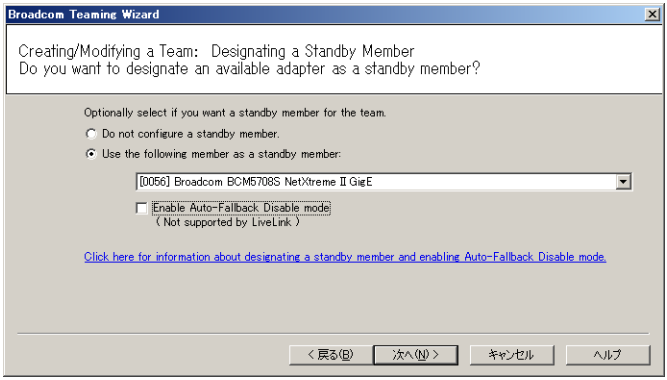
**POINT**

- 少なくとも 1 つのネットワークアダプタをチームに割り当てる必要があります。

Large Send Offload（LSO、大量送信オフロード）および Checksum Offload（CO、チェックサム オフロード）コラムは、アダプタに対して LSO および CO のプロパティがサポートされているか（Y）サポートされていないか（N）を示します。LSO および CO がチームのすべてのメンバについてサポートおよび設定されている場合、LSO および CO プロパティはチームに対して自動的に有効となります。この場合、スクリーンの下部にチームのプロパティが表示されます。



**6 アダプタの 1 つをスタンバイメンバとして指定する場合（オプション）、「Use the following member as a standby member」をクリックします。**



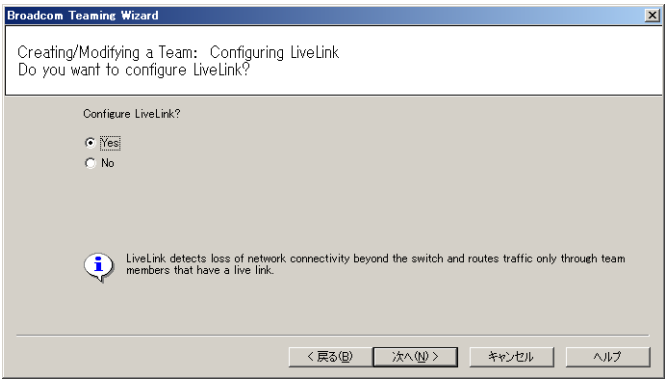

**7 アダプタのリストからスタンバイメンバを選択します。**

自動フォールバックはディスエーブルモード機能によって、プライマリメンバが再びオンラインになったときに、チームはプライマリメンバに切り替えずにスタンバイメンバをそのまま使用できます。この機能を有効にするには、「Enable Auto-Fallback Disable mode」をクリックし、［次へ］をクリックしてください。自動フォールバックはディスエーブルモード機能を有効にした場合、LiveLink は使用できません。

J

**8 LiveLink を設定する場合は、［Yes］を選択し、［次へ］をクリックします。**

LiveLink を設定しない場合は、［No］を選択し、［次へ］をクリックしてください。

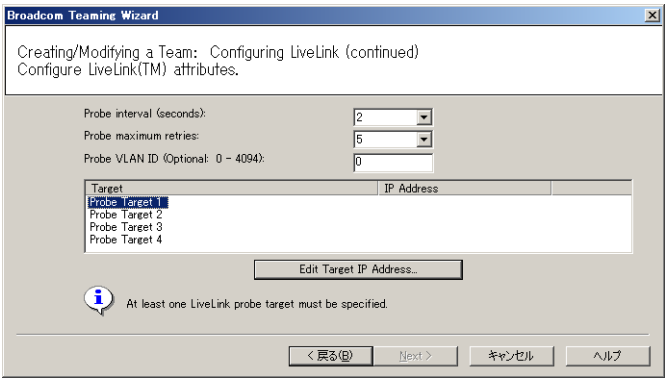



**9 Probe internal（プローブ対象に対するリンクパケットの各再転送間隔の秒数）および Probe maximum retries（フェイルオーバーが発生する前にプローブ対象からの応答を連続して受信しない回数）を設定します。**

**10 リストの最上部にあるプローブ対象をクリックし、「Edit Target IP Address」をクリックして、「IP Address」ボックスに対象 IP アドレスを入力し、［OK］をクリックし、［Next］をクリックします。**

**POINT**

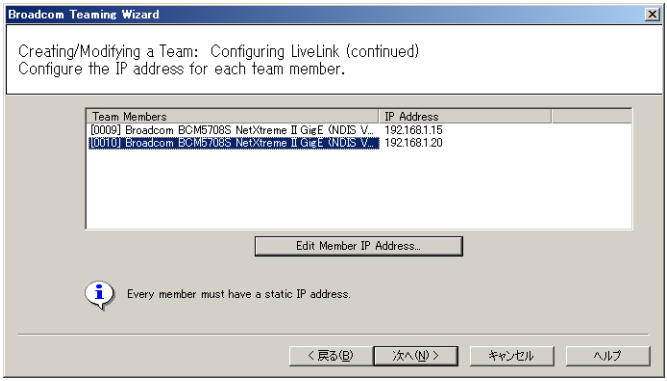
- 1 つ目のプローブ対象のみが必須です。他のプローブ対象に IP アドレスを割り当てることで、プローブ対象を最大 3 個までバックアップとして追加できます。




**11 リストされているチームメンバをクリックし、「Edit Member IP Address」をクリックして、「IP Address」ボックスにメンバ IP アドレスを入力します。リストされているチームメンバすべてに対してこのステップを繰り返し、［OK］をクリックし、［次へ］をクリックします。**

**POINT**

- すべてのメンバ IP アドレスは、プローブ対象のサブネットと同一のサブネットにある必要があります。

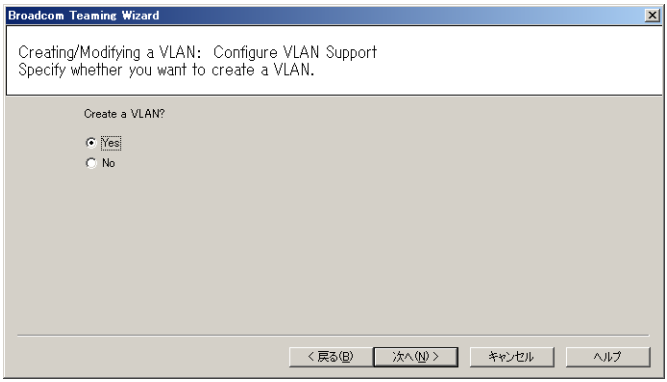



**12 チームに対して VLAN を作成する場合は、［Yes］をクリックし、［次へ］をクリックします。**

チームに対して VLAN を作成しない場合は、［No］をクリックし、［次へ］をクリックして、「完了」スクリーンからウィザードを続行します（手順 17 を参照）。VLAN により、異なるサブネット上にある複数の仮想アダプタを追加できます。複数のサブネットに所属することが可能な 1 つのネットワークアダプタを、利用中のシステムに装備できるようになります。

**POINT**

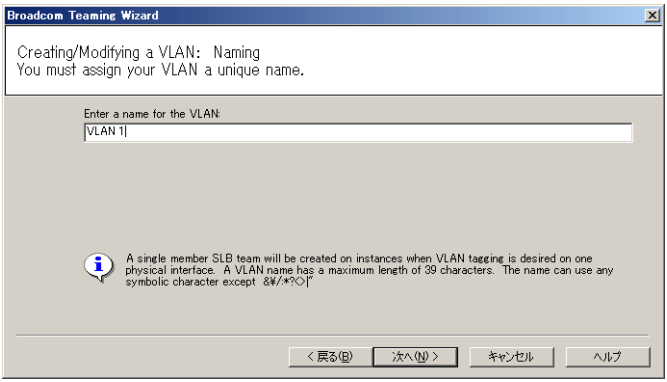
- すべてのチームメンバが Broadcom アダプタでないと VLAN は作成できません。



**13 VLAN 名を入力し、［次へ］をクリックします。**

**POINT**

- チーム名は最大 39 文字で、スペースで開始することはできず、次の文字は使用できません。
  ・& \ / : * ? < > |

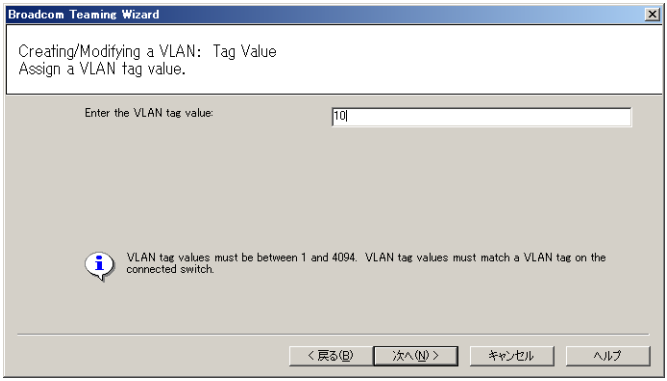



**14 VLAN にタグを付けるには、「Tagged」を選択し、［次へ］をクリックします。**

タグを付けない場合は、「Untagged」を選択し、［次へ］をクリックし、ウィザードを続行してその他の VLAN を追加します（手順 16 を参照）。

**15 VLAN タグ値を入力し、［次へ］をクリックします。**

値は、1 ～ 4094 で設定してください。

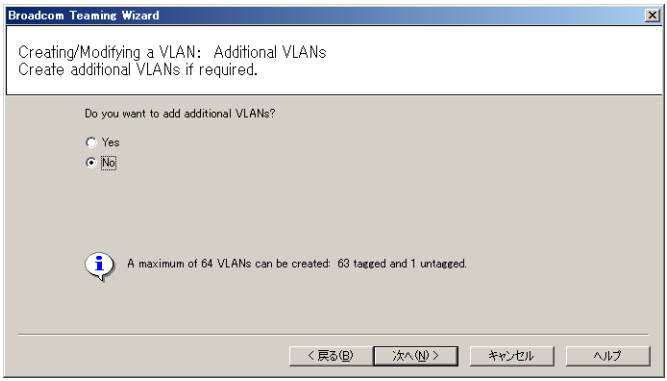



**16 ［Yes］をクリックして別の VLAN を追加し、［次へ］をクリックします。**

必要な VLAN の追加が完了するまで繰り返してください。

**POINT**

- 1 つのチームには、64 個まで VLAN を定義することができます（タグ付けされた VLAN63 個、タグ付けされていない VLAN1 個）。複数の VLAN を追加すると、各 VLAN のメモリおよびプロセッサ時間の使用によって、Windows インタフェースの応答時間が遅くなる場合があります。Windows のパフォーマンスが影響を受ける程度は、システムの設定によって異なります。




J

**17 チームの変更を適用し、確定するには、「Commit changes and return to Broadcom Advanced Control Suite 2」を選択し、［Finish］をクリックします。**

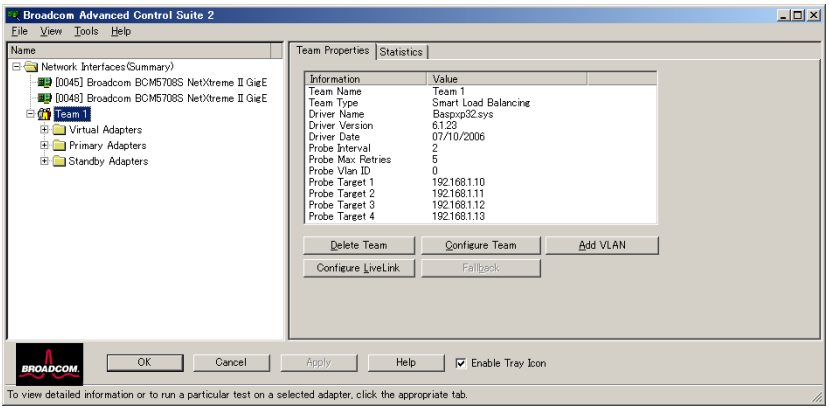
BACS2 でチームの変更をプレビューするには、「Preview changes in Broadcom Advanced Control Suite 2」をクリックし、［Finish］をクリックしてください。
ウィザードが終了し、BACS2 が開きます。

Broadcom Teaming Wizard
Congratulations! The Teaming Wizard has finished collecting information.
How would you like to proceed?
Commit changes and return to Broadcom Advanced Control Suite 2
Preview changes in Broadcom Advanced Control Suite 2
< 戻る(B)
Finish
キャンセル
ヘルプ

**18 ［Finish］をクリックして変更を確定します。**

変更を破棄する場合は、［Cancel］をクリックしてください。

チームをクリックすると、「統計」タブにチームの統計が、「Team Properties」タブにチームのプロパティが表示されます。VLAN をクリックすると、「Vital Signs」タブに VLAN のプロパティが表示されます。



## 5.5.3　エキスパートモードを使用する

チームの作成、チームの変更、VLAN の追加、Smart Load Balance および Failover チームの LiveLink の設定を行うには、エキスパートモードを使用してください。ウィザードを使用してチームを作成するには、「5.5.2 チーム化ウィザードを使用してチームを作成および変更する」（→ P.83）を参照してください。BACS2 の「ツール」メニューからチーム化ウィザードに切り替えるには、「カスタマイズ」をクリックします。「Default Teaming Mode」タブを選択し、「Wizard Mode」を選択します。

### ■チームの作成方法

**POINT**

- SLB（スマートロードバランス）チームのメンバには、ダイナミックホストコンフィギュレーションプロトコル（DHCP）を有効にすることはお勧めしません。

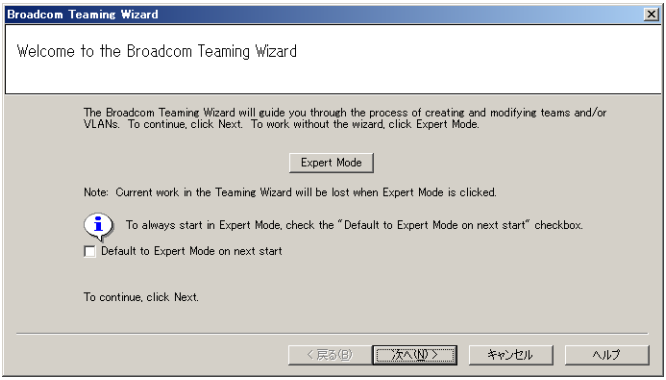
**1　BACS2 の「Tools」メニューから「Create a Team」をクリックします。**

ウィザードの初期画面が表示されます。

**2　ウィザードなしで設定するには、「Expert Mode」をクリックします。**

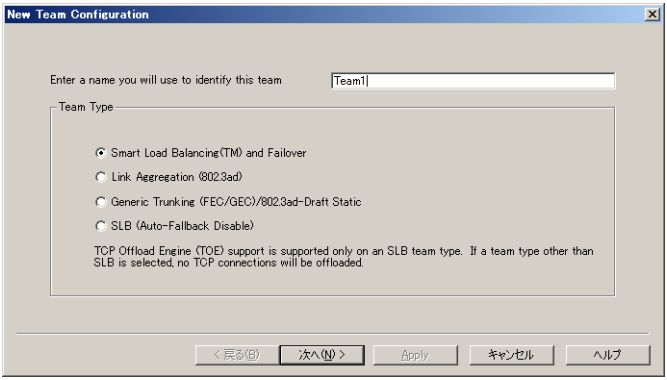
**POINT**

- 常にエキスパートモードを使用してチームを作成する場合は、「Default to Expert Mode on next start」をチェックして、［次へ］をクリックします。


Broadcom Teaming Wizard
Welcome to the Broadcom Teaming Wizard
The Broadcom Teaming Wizard will guide you through the process of creating and modifying teams and/or VLANs. To continue, click Next. To work without the wizard, click Expert Mode.
Expert Mode
Note: Current work in the Teaming Wizard will be lost when Expert Mode is clicked.
To always start in Expert Mode, check the "Default to Expert Mode on next start" checkbox.
Default to Expert Mode on next start
To continue, click Next.
< 戻る(B)
次へ(N) >
キャンセル
ヘルプ

J

3 「Enter a name you will use to identify this team」ボックスにチーム名を入力し、チームタイプを選択し、［次へ］をクリックします。

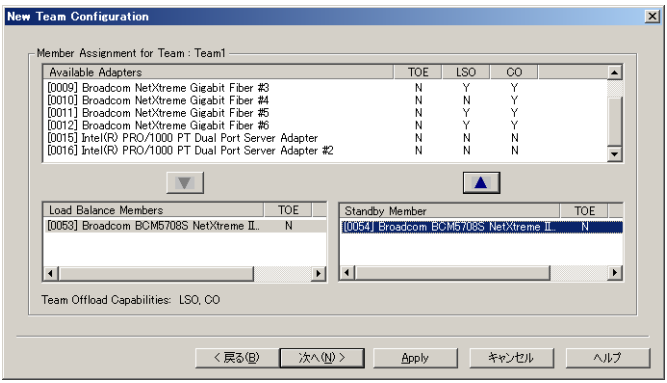

New Team Configuration
Enter a name you will use to identify this team
Team1
Team Type
Smart Load Balancing(TM) and Failover
Link Aggregation (802.3ad)
Generic Trunking (FEC/GEC)/802.3ad-Draft Static
SLB (Auto-Fallback Disable)
TCP Offload Engine (TOE) support is supported only on an SLB team type. If a team type other than SLB is selected, no TCP connections will be offloaded.
< 戻る(B)
次へ(N) >
Apply
キャンセル
ヘルプ

4 「Available Adapters」リストから「Load Balance Members」リストにアダプタを移動して、利用可能な 1 つまたは複数のアダプタをチームに割り当てます。「Load Balance Members」リストには、少なくとも 1 つのアダプタを指定してください。

5 「Load Balance Members」リストから「Standby Member」にアダプタを移動して、利用可能な 1 つまたは複数のアダプタをチームに割り当て、［Apply］をクリックします。

**POINT**

- 少なくとも 1 つのネットワークアダプタをチームに割り当てる必要があります。


New Team Configuration
Member Assignment for Team : Team1
Available Adapters
TOE
LSO
CO
[0009] Broadcom NetXtreme Gigabit Fiber #3 N Y Y
[0010] Broadcom NetXtreme Gigabit Fiber #4 N N Y
[0011] Broadcom NetXtreme Gigabit Fiber #5 N Y Y
[0012] Broadcom NetXtreme Gigabit Fiber #6 N Y Y
[0015] Intel(R) PRO/1000 PT Dual Port Server Adapter N N N
[0016] Intel(R) PRO/1000 PT Dual Port Server Adapter #2 N N N
Load Balance Members
TOE
[0053] Broadcom BCM5708S NetXtreme II... N
Standby Member
TOE
[0054] Broadcom BCM5708S NetXtreme II... N
Team Offload Capabilities: LSO, CO
< 戻る(B)
次へ(N) >
Apply
キャンセル
ヘルプ

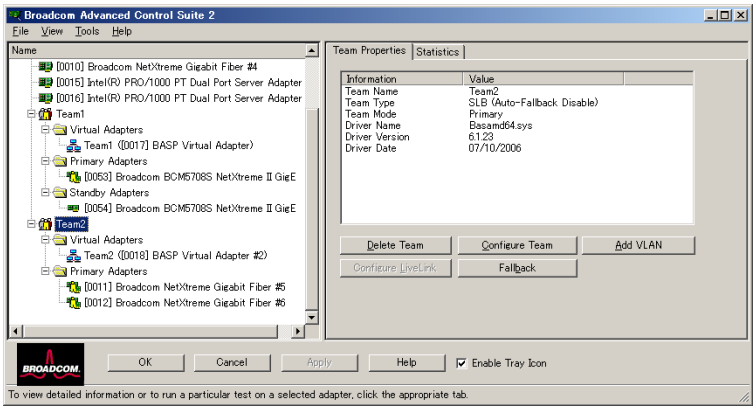
6 ネットワーク接続に一時的な割り込みが発生したというメッセージが表示されたら、［Yes］をクリックします。

**POINT**

- チーム名は最大 39 文字で、スペースで開始することはできず、以下の文字は使用できません。
  ・& \ / : * ? < > |
- チーム名は一意の名前にする必要があります。すでに使用しているチーム名を再度指定しようとすると、名前がすでに存在していることを示すエラーメッセージが表示されます。
- 1 チームの最大メンバ数は 8 個です。
- チームの設定が正しく実行されると、設定が済んだそれぞれのチームに仮想チームアダプタドライバが 1 つずつ作成されます。

・通有中継チームとリンク集約チームを作成した場合は、スタンバイメンバを指定できません。スタンバイメンバは、スマートロードバランスおよびフェイルオーバーチームかスマートロードバランス（自動フォールバックはディスエーブル）チームでのみ動作します。

・スマートロードバランス（自動フォールバックはディスエーブ）チームについては、スタンバイメンバから Load Balance メンバへのトラフィックを復元する場合、「Team Properties」タブの［Fallback］ボタンをクリックします。




## 7 チーム IP アドレスを設定します。

1. 「コントロールパネル」→「ネットワーク接続」の順にクリックします。
2. 設定するチームの名前を右クリックし、「プロパティ」をクリックします。
3. 「全般」タブで、「インターネットプロトコル（TCP/IP）」をクリックし、「プロパティ」をクリックします。
4. そのチームについて、IP アドレスや他に必要な TCP/IP コンフィギュレーションを設定し、［OK］をクリックします。

## ■チームの変更方法

次の方法でチームを変更できます。

・チームタイプの変更
・チームに割り当てられたメンバの変更
・VLAN の追加
・VLAN の変更（エキスパートモードを使用）
・チームまたは VLAN の削除（エキスパートモードを使用）

次にチームの変更方法を説明します。

**1 BACS2 の「tools」→「Create a Team」の順にクリックします。**
ウィザードの初期画面が表示されます。

**2 ［Next］をクリックしてウィザードを使用してチームの変更を続行するか［Expert Mode］をクリックしてエキスパートモードで操作します。**

**3 必要な変更を行ったら、［OK］をクリックします。**

**4 ［Apply］をクリックします。**

**5 ネットワーク接続に一時的な割り込みが発生したというメッセージが表示されたら、［Yes］をクリックします。**

## ■VLAN の追加方法

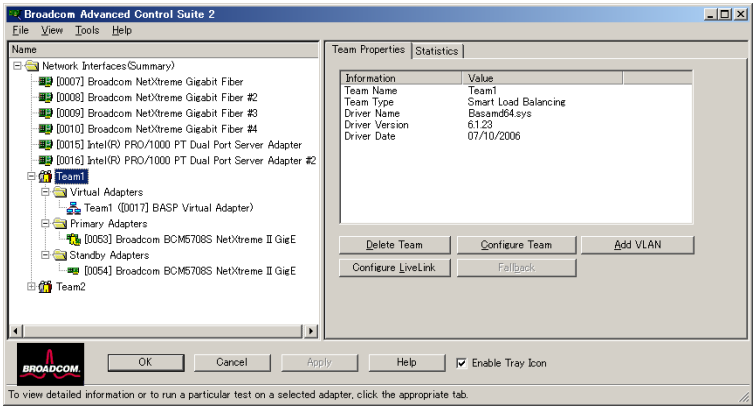
チームには複数の仮想 LAN（VLAN）を追加できます。これにより、異なるサブネット上にある複数の仮想アダプタを追加できます。複数のサブネットに所属することが可能な 1 つのネットワークアダプタを、利用中のシステムに装備できるようになります。VLAN を利用すると、Load Balance メンバのロードバランシング機能が連結でき、フェイルオーバーアダプタも採用できるようになります。

1 つのチームには、64 個まで VLAN を定義できます（タグ付けされた VLAN 63 個、タグ付けされていない VLAN1 個）。ただし、すべてのチームメンバが Broadcom アダプタでないと VLAN は作成できません。Broadcom 以外のアダプタで VLAN を作成しようとすると、エラーメッセージが表示されます。

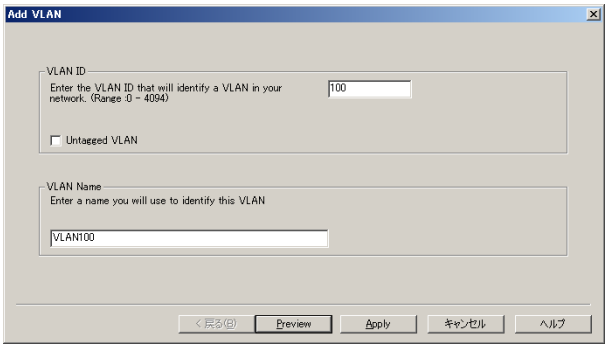
VLAN 環境でチームを設定する方法を説明します。

**1　設定するチームの名前をクリックします。**

**2　「Team Properties」タブで、［Add VLAN］をクリックします。**




**3　「VLAN ID」と「VLAN Name」を入力し、［Apply］をクリックします。**




**POINT**

- すでに存在する VLAN 名や VLAN ID を入力すると、エラーメッセージが表示されます。

**4 ネットワーク接続に一時的な割り込みが発生したというメッセージが表示されたら、［はい］をクリックします。**

**POINT**

- アダプタ性能を最適な状態に保つためには、アダプタごとに作成される 8 つの VLAN それぞれに、64MB のシステムメモリが必要です。

## ■VLAN プロパティの表示および VLAN テストの実行方法

VLAN プロパティの表示および VLAN テストを実行する方法を説明します。

**1 目的の VLAN アダプタの名前をクリックします。**

**2 VLAN アダプタのプロパティを表示するには、「Vital Sign」タブをクリックします。**

**3 VLAN アダプタのネットワークテストを実行するには、「Network Test」タブをクリックします。**

## ■VLAN の削除方法

VLAN を削除するには、削除する VLAN を右クリックし、「Remove VLAN」を選択します。

**1 ［ツール］→「チームの設定」の順にクリックします。**
複数のチームがある場合は、削除対象の VLAN が所属するチームの名前をクリックし、［OK］をクリックしてください。

**2 ［Remove VLAN］をクリックします。**

**3 ［Apply］をクリックします。**
ネットワーク接続に一時的な割り込みが発生したというメッセージが表示されたら、[Yes］をクリックします。

**POINT**

- チームを削除すると、そのチームに設定されている VLAN もすべて削除されます。

## ■Smart Load Balancing（スマート ロード バランス）およびフェイルオーバーチームの LiveLink 設定方法

LiveLink を設定する前に、次の事項をお読みください。

**POINT**

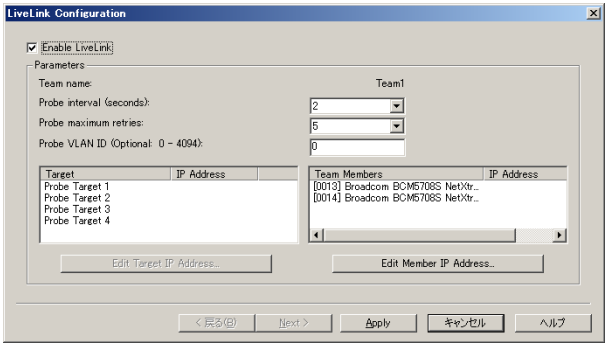
- LiveLink™ を設定する前に、「LiveLink」の説明をお読みください。また、指定するプローブの各対象が利用可能かつ動作していることも確認してください。プローブ対象となる IP アドレスが何らかの理由で変更された場合、LiveLink を再設定する必要があります。何らかの理由でプローブ対象の MAC アドレスが変わった場合、チームを再起動する必要があります（→「4.8.10 チーム化に関する問題のトラブルシューティング」(P.51)）。
- プローブ対象は、チームと同じサブネット上にあり、有効（ブロードキャスト、マルチキャスト、ユニキャストではない）で静的な IP アドレスを割り当てられ、どのような場合でも使用できる（常時オンの状態）必要があります。
- プローブ対象にネットワークが接続されていることを確認するために、チームから ping コマンドを使いプローブの対象を調べます。
- 最大 4 個のプローブ対象を指定することができます。
- プローブ対象またはチームメンバに割り当てられる IP アドレスでは、最初または最後の 8 ビットにゼロを指定できません。

LiveLink を設定する方法について説明します。

**1 Smart Load Balance および Failover（SLB）チームの名前を右クリックし、「Configure LiveLink」をクリックします。**

**2 「Enable LiveLink」ボックスをオンにします。**

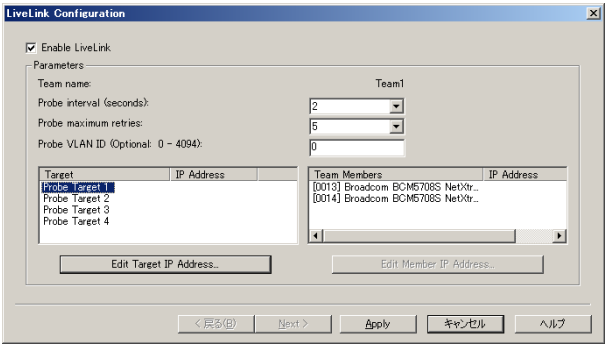
「Probe Interval」（プローブ対象に対するリンク パケットの各再転送間隔の秒数）および「Probe maximum retries」（フェイルオーバーが発生する前にプローブ対象からの応答を連続して受信しない回数）のデフォルト値をそのまま利用することをお勧めします。異なる値を指定するには、「Probe Interval（seconds）」リストからプローブのインターバル、「Probe maximum retries」リストからプローブの最大再送回数をそれぞれ選択します。




**3 リストの最上部にある Probe Target をクリックし、「Edit Target IP Address」をクリックして、「IP Address」ボックスに対象 IP アドレスを入力し、［OK］をクリックします。**

**POINT**

- 1 つ目のプローブ対象のみが必須です。他のプローブ対象に IP アドレスを割り当てることで、プローブ対象を最大 3 個までバックアップとして追加できます。




**4 リストからいずれかのチーム メンバを選択し、「Edit Target IP Address」をクリックして、「IP Address」ボックスにメンバ IP アドレスを入力し、［OK］をクリックします。**

**POINT**

- すべてのメンバ IP アドレスは、プローブ対象のサブネットと同一のサブネットにある必要があります。

**5 手順 4 を繰り返し、リストにある他のチーム メンバの設定を行います。**

**6 ［Apply］をクリックします。**

## ■VLAN（タグ付けされた環境）で LiveLink を設定する方法

### ⚠注意

・VLAN（LiveLink が有効の状態）を使用するチームの場合、プローブ対象と通信するには、プローブ対象とチームの両方がタグなし VLAN（VLAN ID が 0）上にあることが必要です。そうでない場合、チームは接続できません。

**1 チームがタグなし VLAN（VLAN ID が 0）を使用していることを確認してください。**

**2 また、チームとプローブ対象間のネットワーク接続がタグなし VLAN 上で確立されていることを確認してください。**

**3 VLAN を使用している SLB チームの名前を右クリックし、［Configure LiveLink］をクリックします。**

**4 「Enable LiveLink」ボックスをオンにします。**

**5 「Probe interval (seconds)」リストから、プローブのインターバル（プローブ対象へのリンクパケットの各再転送間隔の秒数）をクリックします。**

**6 「Probe maximum retries」リストからプローブの最大再送回数をクリックします。**

**7 リストの最上部にある Probe Target をクリックし、「Edit Target IP Address」をクリックして、「IP Address」ボックスに対象 IP アドレスを入力し、［OK］をクリックします。**

POINT

- 複数のプローブ対象を指定する必要はありません。複数のプローブ対象を指定する場合（最大 4 個まで追加可能）、リストに表示されている次のプローブ対象を選択し、「IP Address」ボックスに対象 IP アドレスを入力して、［OK］をクリックします。

**8 リストからいずれかのチームメンバを選択し、[Edit Target IP Address] をクリックして、「IP Address」ボックスにメンバ IP アドレスを入力し、［OK］をクリックします。**

POINT

- すべてのメンバ IP アドレスは、プローブ対象のサブネットと同一のサブネットにある必要があります。

**9 手順 8 を繰り返し、リストにある他のチームメンバの設定をします。**

**10 ［Apply］をクリックします。**

## ■チームプロパティと統計の表示方法

チームプロパティと統計を表示する方法を説明します。

**1 新しく作成したチームの名前をクリックします。**

**2 「Statistics」タブをクリックして、チームの統計を表示します。**

## ■設定の保存と復元

設定を保存する方法を説明します。

**1 「File」→「Team Save as」の順にクリックします。**

**2 新しい設定ファイルのパスと名前を入力し、「保存」をクリックします。**

ファイル名には .bcg 拡張子が付加されます。
この設定ファイルはテキストファイルです。このため、どんなテキストエディタでも表示できます。このファイルには、アダプタとチーム設定に関する情報が格納されます。

設定を復元する方法について説明します。

**1 「File」→「Team Restore」の順にクリックします。**

**2 復元するファイルの名前をクリックし、［開く］をクリックします。**

**POINT**

- 必要に応じて、ファイルが保存されているフォルダに移動してください。

**3 ［Apply］をクリックします。**

**4 ネットワーク接続に一時的な割り込みが発生したというメッセージが表示されたら、［はい］をクリックします。**

設定がすでにロードされている場合は、現在の設定を保存するかどうかを確認するメッセージが表示されます。現在の設定を保存するには、［Yes］をクリックします。保存しないと、現在ロードされている設定データは失われます。

# Before Reading This Manual

Thank you for purchasing the PRIMERGY 1Gbit/s Ethernet I/O Module (hereinafter referred to as this product or the card).
The card can be installed in the expansion card slot of the Fujitsu server blade to configure the Local Area Network (LAN) system. This manual explains the 1Gbit/s Ethernet I/O Modules and the LAN driver (for Windows). Read this manual carefully to handle the product correctly.
For details about the LAN driver, refer to manuals supplied with the server blade or the Fujitsu PRIMERGY website:
(http://primergy.fujitsu.com)

May, 2007

**For Your Safety**

This manual contains important information, required to operate this product safely.
Thoroughly review the information in this manual before using this product. Especially note the points under "Safety", and only operate this product with a complete understanding of the material provided.
This manual should be kept in an easy-to-access location for quick reference when using this product.

**High Safety**

The Products are designed, developed and manufactured as contemplated or general use, including without limitation, general office use, personal use, household use, and ordinary industrial use, but are not designed, developed and manufactured as contemplated for use accompanying fatal risks or dangers that, unless extremely high safety is secured, could lead directly to death, personal injury, severe physical damage, or other loss (hereinafter "High Safety Required Use"), including without limitation, nuclear reaction control in nuclear facility, aircraft flight control, air traffic control, mass transport control, medical life support system, missile launch control in weapon system. You shall not use this Product without securing the sufficient safety required for the High Safety Required Use. If you wish to use this Product for High Safety Required Use, please consult with our sales representatives in charge before such use.

# Remarks

## Warning Descriptions

Various symbols are used throughout this manual. These are provided to emphasize important points for your safety and that of others. The symbols and their meanings are as follows. Make sure to fully understand these before reading this manual.

| | |
|---|---|
| ⚠ WARNING | Ignoring this symbol could be potentially lethal. |
| ⚠ CAUTION | Ignoring this symbol may lead to injury and/or damage this product. |

The following symbols are used to indicate the type of warning or cautions being described.

| | |
|---|---|
| ⚠ | The triangle mark emphasizes the urgency of the WARNING and CAUTION.<br>Details are described next to the triangle. |
| ⃠ | A barred circle (⃠) warns against certain actions (Do Not).<br>Details are described next to the circle. |
| ● | A black circle indicates actions that must be taken.<br>Details are described next to the black circle. |

## Symbols

The following are symbols used throughout this manual.

| Symbols | Definition |
|---|---|
| IMPORTANT | These sections explain prohibited actions and points to note when using this product. Make sure to read these sections. |
| POINT | These sections explain information needed to operate the hardware and software properly. Make sure to read these sections. |
| → | This mark indicates reference pages or manuals. |

## Entering commands (Keys)

CD-ROM drive names are shown as [CD-ROM drive]. Enter your drive name according to your environment.

[CD-ROM drive]:\Setup.exe

## Abbreviations

The following expressions and abbreviations are used to describe the product names used in this manual.

<table>
<tr><th>Product names</th><th colspan="2">Expressions and abbreviations</th></tr>
<tr><td>1Gbit/s Ethernet I/O Module (PG-LND201)</td><td colspan="2">this product</td></tr>
<tr><td>PG-LND201 LAN Driver</td><td colspan="2">LAN driver or the driver</td></tr>
<tr><td>Microsoft® Windows Server® 2003, Standard Edition</td><td rowspan="4">Windows Server 2003</td><td rowspan="12">Windows</td></tr>
<tr><td>Microsoft® Windows Server® 2003, Enterprise Edition</td></tr>
<tr><td>Microsoft® Windows Server® 2003 R2, Standard Edition</td></tr>
<tr><td>Microsoft® Windows Server® 2003 R2, Enterprise Edition</td></tr>
<tr><td>Microsoft® Windows Server® 2003, Standard x64 Edition</td><td rowspan="4">Windows Server 2003 x64</td></tr>
<tr><td>Microsoft® Windows Server® 2003, Enterprise x64 Edition</td></tr>
<tr><td>Microsoft® Windows Server® 2003 R2, Standard x64 Edition</td></tr>
<tr><td>Microsoft® Windows Server® 2003 R2, Enterprise x64 Edition</td></tr>
<tr><td>Microsoft® Windows® 2000 Server</td><td rowspan="2">Windows 2000 Server</td></tr>
<tr><td>Microsoft® Windows® 2000 Advanced Server</td></tr>
<tr><td>Red Hat® Enterprise Linux® ES (v.3 for x86)</td><td colspan="2" rowspan="10">Linux</td></tr>
<tr><td>Red Hat® Enterprise Linux® AS (v.3 for x86)</td></tr>
<tr><td>Red Hat® Enterprise Linux® AS (v.4 for x86)</td></tr>
<tr><td>Red Hat® Enterprise Linux® ES (v.4 for x86)</td></tr>
<tr><td>Red Hat® Enterprise Linux® AS (v.4 for EM64T)</td></tr>
<tr><td>Red Hat® Enterprise Linux® ES (v.4 for EM64T)</td></tr>
<tr><td>Red Hat® Enterprise Linux® 5 (for x86)</td></tr>
<tr><td>Red Hat® Enterprise Linux® 5 (for Intel64)</td></tr>
<tr><td rowspan="2">PRIMERGY BX620 S3 Server Blade</td><td>BX620 S3 Server Blade</td><td rowspan="2">Server Blade</td></tr>
<tr><td rowspan="2">PRIMERGY BX620 S4 Server Blade</td><td>BX620 S4 Server Blade</td></tr>
<tr><td>PRIMERGY BX600 S3 Blade Server System Unit</td><td colspan="2" rowspan="2">Chassis</td></tr>
<tr><td>PRIMERGY BX600 S2 Blade Server System Unit</td></tr>
<tr><td>Switch Blade</td><td colspan="2" rowspan="2">Switch Blade</td></tr>
<tr><td>Catalyst Blade Switch 3040</td></tr>
<tr><td>FC Pass-Thru Blade</td><td colspan="2">FC Pass-Thru Blade</td></tr>
<tr><td>FC Switch Blade (PG-FCS103/PG-FCS102)</td><td colspan="2">FC Switch Blade</td></tr>
</table>

# Safety

For safe use of this product, it is vital that the following warnings are heeded.

## Handling this product

### ⚠ WARNING

- Do not tinker with the product. Doing so may cause fire or electric shock.
- Keep this product away from water. Failure to do so may cause fire or electric shock.

- When there is lightning nearby, unplug all power cords and external connecting cords from this product. Failure to do so may cause destruction of the devices and fire.

### ⚠ CAUTION

- Since this product is delicate, avoid using or storing it under extreme conditions, such as excessively high or low temperature, high humidity, or in direct sunlight. Do not bend or damage the card or subject it to extreme shock. Doing so may cause failure or fire.

## Recycle

When scrapping this product, contact an office listed in "Appendix A Contact Information" (→pg.195). This product must be disposed of as industrial waste.

# Checking the Items Supplied

Before using the product, check that no supplied or attached items are missing.
If any items are missing, contact an office listed in "Appendix A Contact Information" (→pg.195).

- **1Gbit/s Ethernet I/O Module**
- **User's Guide (this manual)**
- **Screw (3 screws)**

Intel is a registered trademark of Intel Corporation in the USA.
Microsoft, Windows, and Windows Server are trademarks or registered trademarks of Microsoft Corporation in the United States and other countries.
Linux is a trademark or registered trademark of Linus Torvalds in the United States and other countries.
Red Hat and all Red Hat-based trademarks and logos are trademarks or registered trademarks of Red Hat, Inc. in the United States and other countries.
Other product names used are trademarks or registered trademarks of their respective manufacturers.
Other products are copyrights of their respective manufacturers.

All Rights Reserved, Copyright© FUJITSU LIMITED 2007

# Contents


**1 1 Gbit/s Ethernet I/O Module . . . . . 106**
1.1 Overview . . . . . 106
1.2 Specifications . . . . . 106
1.3 Functionality and Features . . . . . 107
**2 Installing a 1Gbit/s Ethernet I/O Module . . . . . 115**
2.1 Installing in a Server Blade . . . . . 116
**3 Installing the LAN Driver . . . . . 118**
3.1 Installing the Driver Software . . . . . 118
**4 Broadcom Gigabit Ethernet Teaming Services . . . . . 119**
4.1 Broadcom Gigabit Ethernet Overview . . . . . 119
4.2 Glossary . . . . . 119
4.3 Teaming Concepts . . . . . 121
4.4 Teaming Mechanisms . . . . . 130
4.5 Types of Teams . . . . . 133
4.6 Attributes of the Features Associated with Each Type of Team . . . . 136
4.7 Teaming and Other Advanced Networking Properties . . . . . 138
4.8 General Network Considerations . . . . . 140
4.9 Event Log Messages . . . . . 151
**5 Broadcom Advanced Control Suite 2 (BACS2) . . . . . 156**
5.1 BACS2 Overview . . . . . 156
5.2 Installing the BACS2 . . . . . 158
5.3 Starting BACS2 . . . . . 162
5.4 Setting of BACS2 . . . . . 162
5.5 Configuring Teaming . . . . . 176
**Appendix A Contact Information . . . . . 195**


E

# 1 1 Gbit/s Ethernet I/O Module

This chapter explains the features and specifications of this product.

## 1.1 Overview

This product is an LAN expansion board exclusive to BX620 S3 Server Blade and BX620 S4 Server Blade.
This product has 2 LAN controllers, and provides LAN connection completely separate/ independent of the onboard LAN. The external access is performed via the Switch Blade installed to the network blade slot 3 or 4 (NET3 or NET4) on the chassis.

IMPORTANT

- A server blade installed with this products and a server blade installed with a fibre channel expansion board cannot be installed to the same chassis.
- When a Switch Blade is installed to network blade slot 3 or 4 (NET3 or NET4), a FC Pass-Thru Blade or FC Switch Blade cannot be installed at the same time.

## 1.2 Specifications

| Item | | Specifications |
|---|---|---|
| Product ID | | PG-LND201 |
| Host bus specifications | Interface | PCI-Express (x4) |
| | Data transfer rate | Max. 1 Gbps |
| | Data transfer system | Bus master, DMA |
| External interface | | 1000BASE-T Ethernet (SerDes) Interface |
| Controller LSI | | BCM 5708S |
| Applicable model | | BX620 S3 Server Blade<br>BX620 S4 Server Blade |

# 1.3 Functionality and Features

## 1.3.1 Functional Description

This product is a new class of Gigabit Ethernet (GbE) converged network interface controller (C-NIC) that can simultaneously perform accelerated data networking, storage networking, and high-performance clustering on a standard Ethernet network. The C-NIC offers acceleration for all popular protocols used in the data center, such as:

- TCP Offload Engine (TOE) for accelerating TCP

**POINT**

- Offloading technologies are supported when this product is installed in a system with Windows Server 2003 with Scalable Networking Pack (SNP).

Using the Broadcom teaming software, you can split your network into virtual LANs (VLANs) as well as group multiple network adapters together into teams to provide network load balancing and fault tolerance functionality. For details about teaming, refer to " Broadcom Advanced Server Program (BSAP) Overview" (→pg.109) in "1.3.3 Teaming Function" (→pg.109). For a description of VLANs, refer to "1.3.4 Virtual LAN Function" (→pg.112). For instructions on configuring teaming and creating VLANs on Windows operating systems, refer to "1.3.3 Teaming Function" (→pg.109).

## 1.3.2 Features

The following is a list of this product features:

- TCP Offload Engine (TOE)
- Single-chip solution
  - Standard Ethernet frame size (1518 bytes)
  - PCI Express v1.0A, x4
  - Full fast-path TCP offload
  - Zero copy capable hardware
- Other performance features
  - TCP, IP, UDP checksum
  - TCP segmentation
- Manageability
  - Broadcom Advanced Control Suite2 (BACS2) diagnostic and configuration software suite
  - Supports PXE 2.0 specification
  - Statistics for SNMP MIB II, Ethernet-like MIB, and Ethernet MIB (IEEE Std 802.3z, Clause 30)
  - IPMI support
- Advanced network features
  - Jumbo frames (up to 9 KB)
  - Virtual LANs
  - Flow Control (IEEE Std 802.3x)
  - LiveLink™ (supported in both the 32-bit and 64-bit Windows operating systems)
  - Logical Link Control (IEEE Std 802.2)
- Layer-2 Priority Encoding (IEEE 802.1p)

E

- High-speed on-chip RISC processor
- Up to 4 classes of service (CoS)
- Integrated 96 KB frame buffer memory
- Support for multicast addresses via 128 bits hashing hardware function
- EM64T processor support

## TCP Offload Engine (TOE)

The TCP/IP protocol suite is used to provide transport services for a wide range of applications for the Internet, LAN, and for file transfer. Without TCP Offload Engine, the TCP/IP protocol suite runs on the host CPU, consuming a very high percentage of its resources and leaving little resources for applications. With the use of this product, the TCP/IP processing can be moved to hardware, freeing the CPU for more important tasks such as application processing.

This product's network adapter's TOE function allows simultaneous operations of up to 1024 fully offloaded TCP connections. The TOE support on the adapter significantly reduces the host CPU utilization while preserving the implementation of the operating system stack.

## Broadcom Advanced Control Suite 2 (BACS2)

Broadcom Advanced Control Suite 2 (BACS2), a component of the Broadcom teaming software, is an integrated utility that provides information about each network adapter that is installed in your system.

The BACS2 also enables you to perform detailed tests, diagnostics, and analysis on each adapter, as well as to modify property values and view traffic statistics for each adapter. BACS2 is used on a Windows operating systems to configure teaming and to add VLANs.

## 1.3.3 Teaming Function

### Broadcom Advanced Server Program (BSAP) Overview

Broadcom Advanced Server Program (BASP) is the Broadcom teaming software for Windows Server 2003 and Windows 2000 Server operating systems. BASP runs within the Broadcom Advanced Control Suite 2 (BACS2) utility.

BASP supports four types of teams for Layer 2 teaming:

- Smart Load Balancing and Failover
- Link Aggregation (802.3ad)
- Generic Trunking (FEC/GEC)/802.3ad-Draft Static
- Smart Load Balancing (Auto-Fallback Disable)

**POINT**

- Enabling Windows Server 2003 built-in bridging is not advisable when you are using teaming software.

For more information on network adapter teaming concepts, refer to "4.3 Teaming Concepts" (→pg.121).

### Load Balancing and Fault Tolerance

Teaming provides traffic load balancing and fault tolerance (redundant adapter operation in the event that a network connection fails). When multiple Gigabit Ethernet network adapters are installed in the same system, they can be grouped into teams, creating a virtual adapter.

A team can consist of two to eight network interfaces, and each interface can be designated as a primary interface or a standby interface (standby interfaces can be used only in a Smart Load Balancing™ and Failover type of team, and only one standby interface can be designated per SLB team). If traffic is not identified on any of the adapter team member connections due to failure of the adapter, cable, switch port, or switch (where the teamed adapters are attached to separate switches), the load distribution is reevaluated and reassigned among the remaining team members. In the event that all of the primary adapters are down, the hot standby adapter becomes active. Existing sessions are maintained and there is no impact on the user.

### Types of Teams

The available types of teams for the Windows Server 2003/Windows 2000 Server operating systems are:

- Smart Load Balancing and Failover
  →" Smart Load Balancing™ and Failover"(pg.110)
- Link Aggregation (802.3ad)
  →" Link Aggregation (802.3ad)"(pg.110)
- Generic Trunking (FEC/GEC)/802.3ad-Draft Static
  →" Generic Trunking (FEC/GEC)/802.3ad-Draft Static"(pg.110)
- SLB (Auto-Fallback Disable)
  →" SLB (Auto-Fallback Disable)"(pg.111)

**IMPORTANT**

- Link aggregation is not supported in the Blade Server.

E

## Smart Load Balancing™ and Failover

Smart Load Balancing™ and Failover is the Broadcom implementation of load balancing based on IP flow. This feature supports balancing IP traffic across multiple adapters (team members) in a bidirectional manner. In this type of team, all adapters in the team have separate MAC addresses. This type of team provides automatic fault detection and dynamic failover to other team member or to a hot standby member. This is done independently of Layer 3 protocol (IP, IPX, NetBEUI); it works with existing Layer 2 and 3 switches. No switch configuration (such as trunk, link aggregation) is necessary for this type of team to work.

POINT

- If you do not enable LiveLink™ when configuring SLB teams, disabling Spanning Tree Protocol (STP) at the switch or port is recommended. This minimizes the downtime due to spanning tree loop determination when failing over. LiveLink mitigates such issues.
- IPX balances only on the transmitting side of the team; other protocols are limited to the primary adapter.
- If a team member is linked at 1000 Mbit/s and another team member is linked at 100 Mbit/s, most of the traffic is handled by the 1000 Mbit/s team member.

## Link Aggregation (802.3ad)

This mode supports link aggregation and conforms to the IEEE 802.3ad (LACP) specification. Configuration software allows you to dynamically configure which adapters you want to participate in a given team. If the link partner is not correctly configured for 802.3ad link configuration, errors are detected and noted. With this mode, all adapters in the team are configured to receive packets for the same MAC address. The outbound load-balancing scheme is determined by our BASP driver. The team link partner determines the load-balancing scheme for inbound packets. In this mode, at least one of the link partners must be in active mode.

IMPORTANT

- Link aggregation (802.3ad) is not supported in the Blade Server.

## Generic Trunking (FEC/GEC)/802.3ad-Draft Static

The Generic Trunking (FEC/GEC)/802.3ad-Draft Static type of team is very similar to the Link Aggregation (802.3ad) type of team, in that all adapters in the team are configured to receive packets for the same MAC address. However, the Generic Trunking (FEC/GEC)/802.3ad-Draft Static) type of team, does not provide LACP or marker protocol support. This type of team supports a variety of environments in which the adapter link partners are statically configured to support a proprietary trunking mechanism. For instance, this type of team could be used to support Lucent's OpenTrunk or Cisco's Fast EtherChannel (FEC). Basically, this type of team is a light version of the Link Aggregation (802.3ad) type of team. This approach is much simpler, in that there is not a formalized link aggregation control protocol (LACP). As with the other types of teams, the creation of teams and the allocation of physical adapters to various teams is done statically through user configuration software.

The Generic Trunking (FEC/GEC/802.3ad-Draft Static) type of team supports load balancing and failover for both outbound and inbound traffic.

## SLB (Auto-Fallback Disable)

The SLB (Auto-Fallback Disable) type of team is identical to the Smart Load Balancing™ and Failover type of team, with the exception of when the standby member is active, if a primary member comes back on line, the team continues using the standby member, rather than switching back to the primary member.

All primary interfaces in a team participate in load-balancing operations by sending and receiving a portion of the total traffic. Standby interfaces take over in the event that all primary interfaces have lost their links.

Failover teaming provides redundant adapter operation (fault tolerance) in the event that a network connection fails. If the primary adapter in a team is disconnected because of failure of the adapter, cable, or switch port, the secondary team member becomes active, redirecting both inbound and outbound traffic originally assigned to the primary adapter. Sessions will be maintained, causing no impact to the user.

## Limitations of Smart Load Balancing™ and Failover/SLB (Auto-Fallback Disable) Types of Teams

Smart Load Balancing™ (SLB) is a protocol-specific scheme. The state of support for IP, IPX, and NetBEUI protocols is listed below.

| Operating System | Failover/ Fallback - All Broadcom | | | Failover/ Fallback - Multivendor | | | Load Balance - All Broadcom | | | Load Balance - Multivendor | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Protocol | IP | IPX | Net BE UI | IP | IPX | Net BE UI | IP | IPX | Net BE UI | IP | IPX | Net BE UI |
| Windows Server 2003 | Y | Y | N | Y | N | N | Y | Y | N | Y | N | N |
| Windows Server 2003 with SNP | Y | Y | N | Y | N | N | Y | Y | N | Y | N | N |
| Windows 2000 Server | Y | Y | Y | Y | N | N | Y | Y | N | Y | N | N |

Y = supported, N = not supported

The Smart Load Balancing™ type of team works with all Ethernet switches without having to configure the switch ports to any special trunking mode. Only IP traffic is load-balanced in both inbound and outbound directions. IPX traffic is load-balanced in the outbound direction only. Other protocol packets are sent and received through one primary interface only. Failover for non-IP traffic is supported only for network adapters. The Generic Trunking type of team requires the Ethernet switch to support some form of port trunking mode (for example, Cisco's Gigabit EtherChannel or other switch vendor's Link Aggregation mode). The Generic Trunking type of team is protocol-independent, and all traffic should be load-balanced and fault-tolerant.

**POINT**

- If you do not enable LiveLink™ when configuring teams, disabling Spanning Tree Protocol (STP) at the switch is recommended. This minimizes the downtime due to the spanning tree loop determination when failing over. LiveLink mitigates such issues.

E

### LiveLink™

LiveLink™ is a feature of BASP that is available only for the Smart Load Balancing™ type of teaming. The purpose of LiveLink is to detect link loss beyond the switch and to route traffic only through team members that have a live link. This function is accomplished though the teaming software. The teaming software periodically probes (issues a link packet from each team member) one or more specified target network device(s). The probe target(s) responds when it receives the link packet. If a team member does not detect the response within a specified amount of time, this indicates that the link has been lost, and the teaming software discontinues passing traffic through that team member. Later, if that team member begins to detect a response from a probe target, this indicates that the link has been restored, and the teaming software automatically resumes passing traffic through that team member. LiveLink works only with TCP/IP.

LiveLink™ is supported in both 32-bit and 64-bit Windows operating systems. Refer to the Channel Bonding documentation for similar functionality in Linux Channel Bonding (refer to http://www.redhat.com/docs/manuals/enterprise/RHEL-3-Manual/ref-guide/s1-modules-ethernet.html).

### Teaming and Large Send Offload/Checksum Offload Support

Large Send Offload (LSO) and Checksum Offload are enabled for a team only when all of the members support and are configured for the feature.

## 1.3.4 Virtual LAN Function

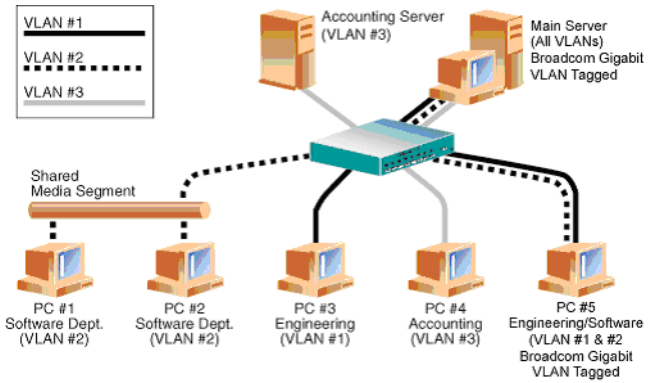
### VLAN Overview

Virtual LANs (VLANs) allow you to split your physical LAN into logical parts, to create logical segmentation of workgroups, and to enforce security policies for each logical segment. Each defined VLAN behaves as its own separate network with its traffic and broadcasts isolated from the others, increasing bandwidth efficiency within each logical group. Up to 64 VLANs (63 tagged and 1 untagged) can be defined for each Broadcom adapter on your server, depending on the amount of memory available in your system.

VLANs can be added to a team to allow multiple VLANs with different VLAN IDs. A virtual adapter is created for each VLAN added.

Although VLANs are commonly used to create individual broadcast domains and/or separate IP subnets, it is sometimes useful for a server to have a presence on more than one VLAN simultaneously. Broadcom adapters support multiple VLANs on a per-port or per-team basis, allowing very flexible network configurations.

• Example of Servers Supporting Multiple VLANs with Tagging




"• Example of Servers Supporting Multiple VLANs with Tagging" (→pg.113)" shows an example network that uses VLANs. In this example network, the physical LAN consists of a switch, two servers, and five clients. The LAN is logically organized into three different VLANs, each representing a different IP subnet. The features of this network are described in "• Example VLAN Network Topology" (→pg.113).

• Example VLAN Network Topology

| Component | Description |
|---|---|
| VLAN #1 | An IP subnet consisting of the Main Server, PC #3, and PC #5. This subnet represents an engineering group. |
| VLAN #2 | Includes the Main Server, PCs #1 and #2 via shared media segment, and PC #5. This VLAN is a software development group. |
| VLAN #3 | Includes the Main Server, the Accounting Server and PC #4. This VLAN is an accounting group. |
| Main Server | A high-use server that needs to be accessed from all VLANs and IP subnets. The Main Server has a Broadcom adapter installed. All three IP subnets are accessed via the single physical adapter interface. The server is attached to one of the switch ports, which is configured for VLANs #1, #2, and #3. Both the adapter and the connected switch port have tagging turned on. Because of the tagging VLAN capabilities of both devices, the server is able to communicate on all three IP subnets in this network, but continues to maintain broadcast separation between all of them. |
| Accounting Server | Available to VLAN #3 only. The Accounting Server is isolated from all traffic on VLANs #1 and #2. The switch port connected to the server has tagging turned off. |
| PCs #1 and #2 | Attached to a shared media hub that is then connected to the switch. PCs #1 and #2 belong to VLAN #2 only, and are logically in the same IP subnet as the Main Server and PC #5. The switch port connected to this segment has tagging turned off. |

E

| Component | Description |
|---|---|
| PC #3 | A member of VLAN #1, PC #3 can communicate only with the Main Server and PC #5. Tagging is not enabled on PC #3 switch port. |
| PC #4 | A member of VLAN #3, PC #4 can only communicate with the servers. Tagging is not enabled on PC #4 switch port. |
| PC #5 | A member of both VLANs #1 and #2, PC #5 has a Broadcom adapter installed. It is connected to switch port #10. Both the adapter and the switch port are configured for VLANs #1 and #2 and have tagging enabled. |

**POINT**

- VLAN tagging is only required to be enabled on switch ports that create trunk links to other switches, or on ports connected to tag-capable end-stations, such as servers or workstations with Broadcom adapters.

## Adding VLANs to Teams

Each team supports up to 64 VLANs (63 tagged and 1 untagged). With multiple VLANs on an adapter, a server with a single adapter can have a logical presence on multiple IP subnets. With multiple VLANs in a team, a server can have a logical presence on multiple IP subnets and benefit from load balancing and failover. For instructions on adding a VLAN to a team, refer to "5.5 Configuring Teaming" (→pg.176).

**POINT**

- Adapters that are members of a failover team can also be configured to support VLANs. Because VLANs are not supported for an Intel LOM, if an Intel LOM is a member of a failover team, VLANs cannot be configured for that team.

# 2 Installing a 1Gbit/s Ethernet I/O Module

This chapter explains the installation procedure in the server blade.

**WARNING**

- When installing or removing this product, make sure to remove the server blade from the chassis. Failure to do so may cause electric shock.
  For details on how to remove the server blade from the chassis, refer to "Blade Server System Unit Hardware Guide".

**CAUTION**

- The circuit boards and soldered parts of internal options are exposed. They can be damaged by static electricity. Before handling them, first touch a metal part of the server blade to discharge static electricity from your body.
- Do not touch the circuitry on boards or soldered parts. Hold the metallic areas or the edges of the circuit boards.
- These products are susceptible to static electricity. Place them on conductive pads or keep them in their packaging as long as they are not necessary.

E

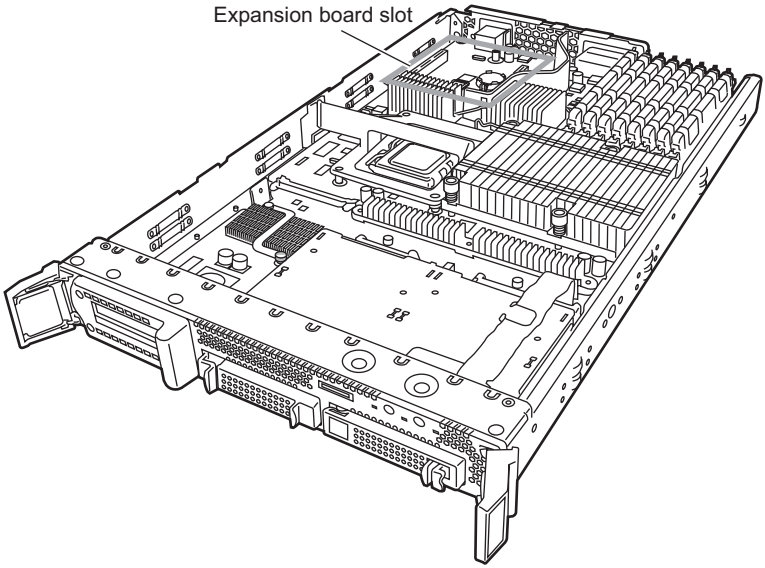
# 2.1 Installing in a Server Blade

**POINT**

- To connect a 1Gbit/s Ethernet I/O Module to the external LAN (device), it is necessary to install a Switch Blade or GbE Pass-Thru Blade to network blade slot 3 or network blade slot 4 (NET3 or NET4) of the chassis.

## 2.1.1 Installation Position of the 1Gbit/s Ethernet I/O Module

Install the 1Gbit/s Ethernet I/O Module in the expansion board slot in the BX620 S3/BX620 S4 Server Blade.




## 2.1.2 Installation Procedure for the 1Gbit/s Ethernet I/O Module

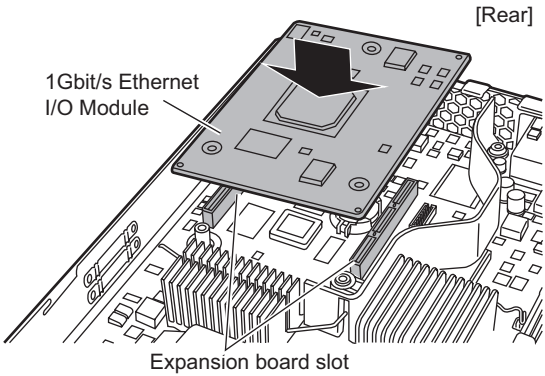
1. **Turn off the server blade where the 1Gbit/s Ethernet I/O Module will be installed.**
   → "3.3 Turning Off the Server " in "Blade Server System Unit Hardware Guide"
2. **Touch a metal part of the chassis to discharge static electricity from your body.**
3. **Remove the server blade from the chassis.**
   →"4.2 Installing Server Blades" in "Blade Server System Unit Hardware Guide"

### 4 Remove the top cover.

→"7.2 Removing and Attaching the Top Cover" in "Server Blade User's Guide"

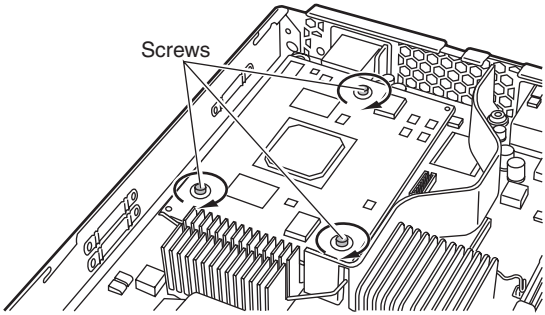
### 5 Install the 1Gbit/s Ethernet I/O Module.

Make sure the 1Gbit/s Ethernet I/O Module is securely on the slot.




### 6 Secure the 1Gbit/s Ethernet I/O Module with the screws.

Secure the 1Gbit/s Ethernet I/O Module with the three screws included with this product.




### 7 Attach the top cover.

→"7.2 Removing and Attaching the Top Cover" in "Server Blade User's Guide"

### 8 Install the server blade to the chassis.

→"4.2 Installing Server Blades" in "Blade Server System Unit Hardware Guide"

E

# 3 Installing the LAN Driver

This chapter explains how to install the LAN driver.

## 3.1 Installing the Driver Software

**POINT**

- Get the LAN driver from the ServerStart CD-ROM included with the BX620 S4 server blade and install.
  If using a LAN driver, refer to the operation manual or help file included with the driver.
- Do not use LAN drivers downloaded from Broadcom's online service in the PRIMERGY server.
- Before installing the driver software, verify that the Windows operating system has been upgraded to the latest version with the latest service pack applied.
- To use TCP/IP Offload Engine (TOE), you must have Windows Server 2003 with Scalable Networking Pack (SNP)

### 3.1.1 Installing the LAN Drivers

The installer will detect if SNP for Windows Server 2003 is installed on your machine. If it is, the installer will install the NDIS 5.2 driver, which is necessary in order to use TOE. If SNP for Windows Server 2003 is not installed on your machine, the installer will install the NDIS 5.1 driver and you will not be able to use TOE.

**1 Insert the ServerStart Disc1 CD-ROM.**

**2 Execute the following EXE file.**

- For Windows Server 2003 x64
  \DRIVERS\LAN\Broadcom\Ext\W2K3x64\DrvInst\setup.exe
- For Windows Server 2003
  \DRIVERS\LAN\Broadcom\Ext\W2K3\DrvInst\setup.exe
- For Windows Server 2000
  \DRIVERS\LAN\Broadcom\Ext\W2K\DrvInst\setup.exe

**3 Click [Next].**

The installation of the LAN driver is started.

**4 Click [Finish].**

**5 Eject the CD-ROM, and restart the server blade.**

# 4 Broadcom Gigabit Ethernet Teaming Services

This chapter explains the technology and considerations when working with the network teaming services.

## 4.1 Broadcom Gigabit Ethernet Overview

The goal of Broadcom teaming services is to provide fault tolerance and link aggregation across a team of two or more adapters. The information in this manual is provided to assist IT professionals during the deployment and troubleshooting of system applications that require network fault tolerance and load balancing.

## 4.2 Glossary

| Item | Definition |
|---|---|
| ARP | Address Resolution Protocol |
| BACS | Broadcom Advanced Control Suite |
| BASP | Broadcom Advanced Server Program (intermediate driver) |
| DNS | Domain Name Service |
| G-ARP | Gratuitous Address Resolution Protocol |
| Generic Trunking (FEC/GEC)/ 802.3ad-Draft Static | Switch-dependent load balancing and failover type of team in which the intermediate driver manages outgoing traffic and the switch manages incoming traffic. |
| HSRP | Hot Standby Router Protocol |
| ICMP | Internet Control Message Protocol |
| IGMP | Internet Group Management Protocol |
| IP | Internet Protocol |
| LACP | Link Aggregation Control Protocol |
| Link Aggregation (802.3ad) | Switch-dependent load balancing and failover type of team with LACP in which the intermediate driver manages outgoing traffic and the switch manages incoming traffic. |
| LOM | LAN on Motherboard |
| MAC | Media Access Control |
| NDIS | Network Driver Interface Specification |
| NLB | Network Load Balancing (Microsoft) |

E

| Item | Definition |
|---|---|
| PXE | Preboot Execution Environment |
| RAID | Redundant Array of Inexpensive Disks |
| Smart Load Balancing™ and Failover | Switch-independent failover type of team in which the primary team member handles all incoming and outgoing traffic while the standby team member is idle until a failover event (for example, loss of link occurs). The intermediate driver (BASP) manages incoming/outgoing traffic. |
| Smart Load Balancing (SLB) | Switch-independent load balancing and failover type of team, in which the intermediate driver manages outgoing/incoming traffic. |
| TCP | Transmission Control Protocol |
| UDP | User Datagram Protocol |
| WINS | Windows name service |
| WLBS | Windows Load Balancing Service |

# 4.3 Teaming Concepts

Storage devices use RAID technology to group individual hard drives. Switch ports can be grouped together using technologies such as Cisco Gigabit EtherChannel, IEEE 802.3ad Link Aggregation, Bay Network Multilink Trunking, and Extreme Network Load Sharing. Network interfaces on servers can be grouped together into a team of physical ports called a virtual adapter.

## 4.3.1 Teaming and Network Addresses

### Network Addressing

To understand how teaming works, it is important to understand how node communications work in an Ethernet network. This Section is based on the assumption that the reader is familiar with the basics of IP and Ethernet network communications. The following information provides the concepts of network addressing used in an Ethernet network.

Every Ethernet network interface in a host platform, such as a computer system, requires a globally unique Layer 2 address and at least one globally unique Layer 3 address. Layer 2 is the Data Link Layer, and Layer 3 is the Network layer as defined in the OSI model. The Layer 2 address is assigned to the hardware and is often referred to as the MAC address or physical address. This address is pre-programmed at the factory and stored in NVRAM on a network interface card or on the system motherboard for an embedded LAN interface. The Layer 3 addresses are referred to as the protocol or logical address assigned to the software stack. IP and IPX are examples of Layer 3 protocols. In addition, Layer 4 (Transport Layer) uses port numbers for each network upper level protocol such as Telnet or FTP. These port numbers are used to differentiate traffic flows across applications. The combination of the IP address and the TCP port number is called a socket.

Ethernet devices communicate with other Ethernet devices using the MAC address, not the IP address. However, most applications work with a host name that is translated to an IP address by a Naming Service such as WINS and DNS. Therefore, a method of identifying the MAC address assigned to the IP address is required. The Address Resolution Protocol for an IP network provides this mechanism. For IPX, the MAC address is part of the network address and ARP is not required. ARP is implemented using an ARP Request and ARP Reply frame. ARP Requests are typically sent to a broadcast address while the ARP Reply is typically sent as unicast traffic. A unicast address corresponds to a single MAC address or a single IP address. A broadcast address is sent to all devices on a network.

### Teaming and Network Addresses

A team of adapters will function as a single virtual network interface, and do not appear to be any different than a non-teamed adapter to other network devices. A virtual network adapter advertises a single Layer 2, and one or more Layer 3 addresses. When the teaming driver initializes, it selects one MAC address from one of the physical adapters that make up the team to be the Team MAC address. This address is typically taken from the first adapter that gets initialized by the driver. When the system hosting the team receives an ARP request, it selects one MAC address from among the physical adapters in the team to use as the source MAC address in the ARP Reply. In Windows operating systems, the IPCONFIG /all command shows the IP and MAC address of the virtual adapter and not the individual physical adapters. The protocol IP address is assigned to the virtual network interface and not to the individual physical adapters.

E

For switch-independent teaming modes, all physical adapters that make up a virtual adapter must use the unique MAC address assigned to them when transmitting data. That is, the frames that are sent by each of the physical adapters in the team must use a unique MAC address to be IEEE compliant. It is important to note that ARP cache entries are not learned from received frames, but only from ARP requests and ARP replies.

## 4.3.2 Types of Teams

"Available Teaming Types" shows a summary of the teaming types and their classification.
Available Teaming Types

| Teaming Type | Switch-Dependent*1 | Link Aggregation Control Protocol Support Required on the Switch | Load Balancing | Failover |
|---|---|---|---|---|
| Smart Load Balancing and Failover | – | – | ❍ | ❍ |
| SLB (Auto-Fallback Disable) | – | – | ❍ | ❍ |
| Link Aggregation (802.3ad) *2 | ❍ | ❍ | ❍ | ❍ |
| Generic Trunking (FEC/GEC)/802.3ad-Draft Static | ❍ | – | ❍ | ❍ |

*1: Switch must support specific type of team.
*2: Link aggregation is not supported in the Blade Server.

### Smart Load Balancing and Failover

The Smart Load Balancing™ and Failover type of team provides both load balancing and failover when configured for load balancing, and only failover when configured for fault tolerance. This type of team works with any Ethernet switch and requires no trunking configuration on the switch. The team advertises multiple MAC addresses and one or more IP addresses (when using secondary IP addresses). The team MAC address is selected from the list of load balance members. When the system receives an ARP request, the software-networking stack will always send an ARP Reply with the team MAC address. To begin the load balancing process, the teaming driver will modify this ARP reply by changing the source MAC address to match one of the physical adapters.

Smart Load Balancing enables both transmit and receive load balancing based on the Layer 3/Layer 4 IP address and TCP/UDP port number. In other words, the load balancing is not done at a byte or frame level but on a TCP/UDP session basis. This methodology is required to maintain in-order delivery of frames that belong to the same socket conversation. Load balancing is supported on 2-8 ports. These ports can include any combination of add-in adapters and LAN on Motherboard (LOM) devices. Transmit load balancing is achieved by creating a hashing table using the source and destination IP addresses and TCP/UDP port numbers.The same combination of source and destination IP addresses and TCP/UDP port numbers will generally yield the same hash index and therefore point to the same port in the team. When a port is selected to carry all the frames of a given socket, the unique MAC address of the physical adapter is included in the frame, and not the team MAC address. This is required to comply with the IEEE 802.3 standard. If two adapters transmit using the same MAC address, then a duplicate MAC address situation would occur that the switch could not handle.

Receive load balancing is achieved through an intermediate driver by sending gratuitous ARPs on a client by client basis using the unicast address of each client as the destination address of the ARP request (also known as a directed ARP). This is considered client load balancing and not traffic load balancing. When the intermediate driver detects a significant load imbalance between the physical adapters in an SLB team, it will generate G-ARPs in an effort to redistribute incoming frames. The intermediate driver (BASP) does not answer ARP requests; only the software protocol stack provides the required ARP Reply. The receive load balancing is a function of the number of clients that are connecting to the system through the team interface.

SLB receive load balancing attempts to load balance incoming traffic for client machines across physical ports in the team. It uses a modified gratuitous ARP to advertise a different MAC address for the team IP Address in the sender physical and protocol address. This G-ARP is unicast with the MAC and IP Address of a client machine in the target physical and protocol address respectively. This causes the target client to update its ARP cache with a new MAC address map to the team IP address. G-ARPs are not broadcast because this would cause all clients to send their traffic to the same port. As a result, the benefits achieved through client load balancing would be eliminated, and could cause out of order frame delivery. This receive load balancing scheme works as long as all clients and the teamed system are on the same subnet or broadcast domain.

When the clients and the system are on different subnets, and incoming traffic has to traverse a router, the received traffic destined for the system is not load balanced. The physical adapter that the intermediate driver has selected to carry the IP flow carries all of the traffic. When the router sends a frame to the team IP address, it broadcasts an ARP request (if not in the ARP cache). The server software stack generates an ARP reply with the team MAC address, but the intermediate driver modifies the ARP reply and send it over a particular physical adapter, establishing the flow for that session.

The reason is that ARP is not a routable protocol. It does not have an IP header and therefore is not sent to the router or default gateway. ARP is only a local subnet protocol. In addition, since the G-ARP is not a broadcast packet, the router will not process it and will not update its own ARP cache.

The only way that the router would process an ARP that is intended for another network device is if it has Proxy ARP enabled and the host has no default gateway. This is very rare and not recommended for most applications.

Transmit traffic through a router will be load balanced as transmit load balancing is based on the source and destination IP address and TCP/UDP port number. Since routers do not alter the source and destination IP address, the load balancing algorithm works as intended.

Configuring routers for Hot Standby Routing Protocol (HSRP) does not allow for receive load balancing to occur in the adapter team. In general, HSRP allows for two routers to act as one router, advertising a virtual IP and virtual MAC address. One physical router is the active interface while the other is standby. Although HSRP can also load share nodes (using different default gateways on the host nodes) across multiple routers in HSRP groups, it always points to the primary MAC address of the team.

## SLB (Auto-Fallback Disable)

This type of team is identical to the Smart Load Balance and Failover type of team, with the following exception-when the standby member is active, if a primary member comes back on line, the team continues using the standby member rather than switching back to the primary member. This type of team is supported only for situations in which the network cable is disconnected and reconnected to the network adapter. It is not supported for situations in which the adapter is removed/installed through Device Manager or Hot-Plug PCI.

If any primary adapter assigned to a team is disabled, the team functions as a Smart Load Balancing and Failover type of team in which auto-fallback occurs.

## Link Aggregation (IEEE 802.3ad LACP)

Link Aggregation is similar to Generic Trunking except that it uses the Link Aggregation Control Protocol to negotiate the ports that will make up the team. LACP must be enabled at both ends of the link for the team to be operational. If LACP is not available at both ends of the link, 802.3ad provides a manual aggregation that only requires both ends of the link to be in a link up state. Because manual aggregation provides for the activation of a member link without performing the LACP message exchanges, it should not be considered as reliable and robust as an LACP negotiated link. LACP automatically determines which member links can be aggregated and then aggregates them. It provides for the controlled addition and removal of physical links for the link aggregation so that no frames are lost or duplicated. The removal of aggregate link members is provided by the marker protocol that can be optionally enabled for Link Aggregation Control Protocol (LACP) enabled aggregate links.

The Link Aggregation group advertises a single MAC address for all the ports in the trunk. The MAC address of the Aggregator can be the MAC addresses of one of the MACs that make up the group. LACP and marker protocols use a multicast destination address.

The Link Aggregation control function determines which links may be aggregated and then binds the ports to an Aggregator function in the system and monitors conditions to determine if a change in the aggregation group is required. Link aggregation combines the individual capacity of multiple links to form a high performance virtual link. The failure or replacement of a link in an LACP trunk will not cause loss of connectivity. The traffic will simply be failed over to the remaining links in the trunk.

IMPORTANT

- Link aggregation is not supported in the Blade Server.

### Generic Trunking

Generic Trunking is a switch-assisted teaming mode and requires configuring ports at both ends of the link: server interfaces and switch ports. This is often referred to as Cisco Fast EtherChannel or Gigabit EtherChannel. In addition, generic trunking supports similar implementations by other switch OEMs such as Extreme Networks Load Sharing and Bay Networks or IEEE 802.3ad Link Aggregation static mode. In this mode, the team advertises one MAC Address and one IP Address when the protocol stack responds to ARP Requests. In addition, each physical adapter in the team uses the same team MAC address when transmitting frames. This is possible since the switch at the other end of the link is aware of the teaming mode and will handle the use of a single MAC address by every port in the team. The forwarding table in the switch will reflect the trunk as a single virtual port.

In this teaming mode, the intermediate driver controls load balancing and failover for outgoing traffic only, while incoming traffic is controlled by the switch firmware and hardware. As is the case for Smart Load Balancing, the BASP intermediate driver uses the IP/TCP/UDP source and destination addresses to load balance the transmit traffic from the server. Most switches implement an XOR hashing of the source and destination MAC address.

## 4.3.3 Software Components

Teaming is implemented via an NDIS intermediate driver in the Windows Operating System environment. This software component works with the miniport driver, the NDIS layer, and the protocol stack to enable the teaming architecture (refer to "• Process for Selecting a Team Type" (→pg.129)). The miniport driver controls the host LAN controller directly to enable functions such as send, receive, and interrupt processing. The intermediate driver fits between the miniport driver and the protocol layer multiplexing several miniport driver instances, and creating a virtual adapter that looks like a single adapter to the NDIS layer. NDIS provides a set of library functions to enable the communications between either miniport drivers or intermediate drivers and the protocol stack. The protocol stack implements IP, IPX and ARP. A protocol address such as an IP address is assigned to each miniport device instance, but when an Intermediate driver is installed, the protocol address is assigned to the virtual team adapter and not to the individual miniport devices that make up the team.

The Broadcom supplied teaming support is provided by three individual software components that work together and are supported as a package. When one component is upgraded, all the other components must be upgraded to supported versions. "• Broadcom Teaming Software Component" (→pg.126) describes the three software components and their associated files for supported operating systems.

E

• Broadcom Teaming Software Component

| Software Component | Broadcom Name | Windows File Name |
|---|---|---|
| – | Virtual Bus Driver (VBD) | bxvbdx.sys<br>bxvbda.sys* |
| Miniport Driver | Broadcom Base Driver | bxnd50x.sys<br>bxnd51x.sys<br>bxnd51a.sys*<br>bxnd52x.sys<br>bxnd52a.sys* |
| Intermediate Driver | Broadcom Advanced Server Program (BASP) | Baspxp32.sys<br>Baspw2k.sys |
| Configuration User Interface | Broadcom Advanced Control Suite 2 (BACS2) | BACS2 |

*: For 64-bit systems

## 4.3.4 Hardware Requirements

The various teaming modes described in this manual place certain restrictions on the networking equipment used to connect clients to teamed systems. Each type of network interconnect technology has an effect on teaming as described in the following sections.

- **Repeater Hub**

  A Repeater Hub allows a network administrator to extend an Ethernet network beyond the limits of an individual segment. The repeater regenerates the input signal received on one port onto all other connected ports, forming a single collision domain. This means that when a station attached to a repeater sends an Ethernet frame to another station, every station within the same collision domain will also receive that message. If two stations begin transmitting at the same time, a collision occurs, and each transmitting station must retransmit its data after waiting a short (random) amount of time.

  The use of a repeater requires that each station participating within the collision domain operate in half-duplex mode. Although half-duplex mode is supported for Gigabit Ethernet adapters in the IEEE 802.3 specification, half-duplex mode is not supported by the majority of Gigabit Ethernet adapter manufacturers. Therefore, half-duplex mode will not be considered here.

  Teaming across hubs is supported for troubleshooting purposes (such as connecting a network analyzer) for SLB teams only.

- **Switching Hub**

  Unlike a repeater hub, a switching hub (or more simply a switch) allows an Ethernet network to be broken into multiple collision domains. The switch is responsible for forwarding Ethernet packets between hosts based solely on Ethernet MAC addresses. A physical network adapter that is attached to a switch may operate in half-duplex or full-duplex mode.

  To support Generic Trunking and 802.3ad Link Aggregation, a switch must specifically support such functionality. If the switch does not support these protocols, it may still be used for Smart Load Balancing.

- **Router**
  A router is designed to route network traffic based on Layer 3 or higher protocols, although it often also works as a Layer 2 device with switching capabilities. The teaming of ports connected directly to a router is not supported.

## 4.3.5 Configuring Teaming

The Broadcom Advanced Control Suite 2 (BACS2) utility is used to configure teaming in the supported operating system environments.

The BACS2 utility is designed to run in one of the following 32-bit and 64-bit Windows operating systems: Microsoft Windows 2000 Server and Windows Server 2003. BACS2 is used to configure load balancing and fault tolerance teaming, and VLANs. In addition, it displays the MAC address, driver version, and status information. BACS2 also includes a number of diagnostics tools such as hardware diagnostics, cable testing, and a network topology test.

## 4.3.6 Supported Features by Team Type

"Comparison of Team Types" provides a feature comparison across the team types. Use this table to determine the best type of team for your application. The teaming software supports up to eight ports in a single team and up to four teams in a single system. The four teams can be any combination of the supported teaming types, but each team must be on a separate network or subnet.

- Comparison of Team Types

| Type of Team | Fault Tolerance | Load Balancing | Switch-Dependent Static Trunking | Switch-Independent Dynamic Link Aggregation (IEEE 802.3ad) |
|---|---|---|---|---|
| Function | SLB with Standby(*1) | SLB | Generic Trunking | Link Aggregation |
| Number of ports per team (same broadcast domain) | 2-8 | 2-8 | 2-8 | 2-8 |
| Number of teams | 4 | 4 | 4 | 4 |
| Adapter fault tolerance | Yes | Yes | Yes | Yes |
| Switch link fault tolerance (same broadcast domain) | Yes | Yes | Switch-dependent | Switch-dependent |
| TX load balancing | No | Yes | Yes | Yes |
| RX load balancing | No | Yes | Yes (performed by the switch) | Yes (performed by the switch) |
| Requires compatible switch | No | No | Yes | Yes |
| Heartbeats to check connectivity | No | No | No | No |

| Type of Team | Fault Tolerance | Load Balancing | Switch-Dependent Static Trunking | Switch-Independent Dynamic Link Aggregation (IEEE 802.3ad) |
|---|---|---|---|---|
| Function | SLB with Standby(*1) | SLB | Generic Trunking | Link Aggregation |
| Mixed media (adapters with different media) | Yes | Yes | Yes (switch-dependent) | – |
| Mixed speeds (adapters that do not support a common speed(s), but can operate at different speeds) | Yes | Yes | No | No |
| Mixed speeds (adapters that support a common speed(s), but can operate at different speeds) | Yes | Yes | No (must be the same speed) | Yes |
| Load balances TCP/IP | No | Yes | Yes | Yes |
| Mixed vendor teaming | Yes(*2) | Yes(*2) | Yes(*2) | Yes(*2) |
| Load balances non-IP | No | Yes (IPX outbound traffic only) | Yes | Yes |
| Same MAC address for all team members | No | No | Yes | Yes |
| Same IP address for all team members | Yes | Yes | Yes | Yes |
| Load balancing by IP address | No | Yes | Yes | Yes |
| Load balancing by MAC address | No | Yes (used for no-IP/IPX) | Yes | Yes |

*1: SLB with one primary and one standby member.

*2: Requires at least one Broadcom adapter in the team.

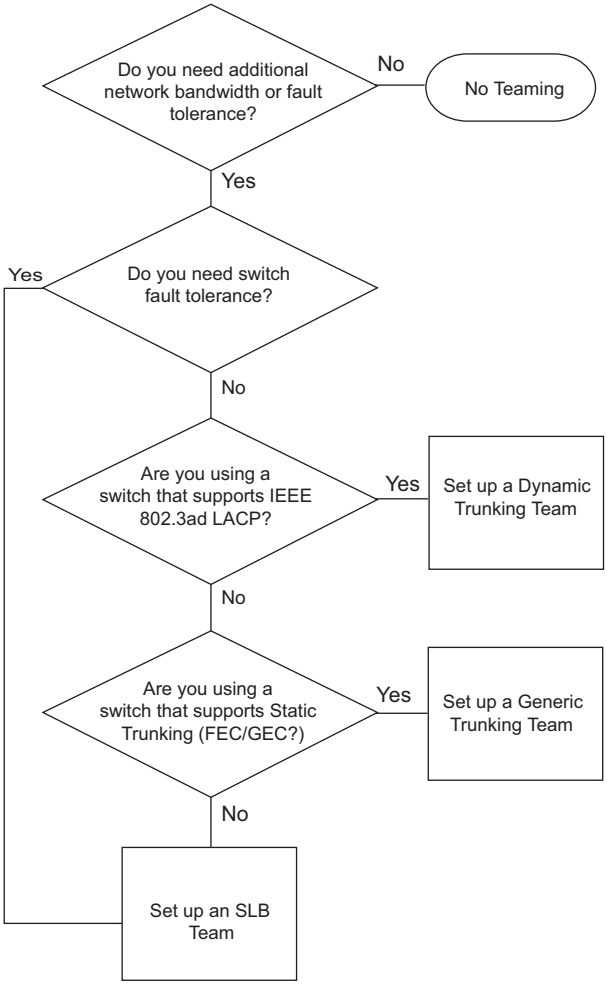
IMPORTANT

- Link aggregation is not supported in the Blade Server.

## 4.3.7 Selecting a Team Type

The following flow chart provides the decision flow when planning for Layer 2 teaming. The primary rationale for teaming is the need for additional network bandwidth and fault tolerance. Teaming offers link aggregation and fault tolerance to meet both of these requirements. Preference teaming should be selected in the following order: IEEE 802.3ad as the first choice, Generic Trunking as the second choice, and SLB teaming as the third choice when using unmanaged switches or switches that do not support the first two options. if switch fault tolerance is a requirement, however, then SLB is the only choice (refer to "• Process for Selecting a Team Type" (→pg.129)).

• Process for Selecting a Team Type

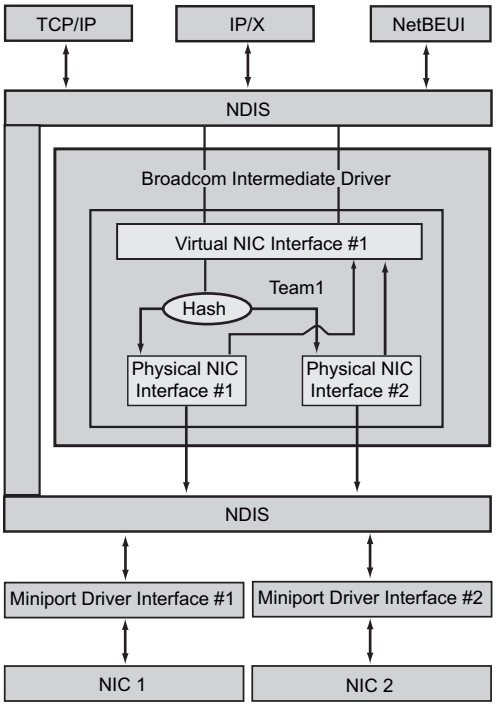


# 4.4 Teaming Mechanisms

## 4.4.1 Architecture

The Broadcom Advanced Server Program (BASP) is implemented as an NDIS intermediate driver (refer to "• Teaming Across Switches Without an Interswitch Link" (→pg.141)). It operates below protocol stacks such as TCP/IP and IPX and appears as a virtual adapter. This virtual adapter inherits the MAC Address of the first port initialized in the team. A Layer 3 address must also be configured for the virtual adapter. The primary function of BASP is to balance inbound (for SLB) and outbound traffic (for all teaming modes) among the physical adapters installed on the system selected for teaming. The inbound and outbound algorithms are independent and orthogonal to each other. The outbound traffic for a particular session can be assigned to a given port while its corresponding inbound traffic can be assigned to a different port.

• Intermediate Driver



## 4.4.2 Outbound Traffic Flow

The Broadcom Intermediate Driver manages the outbound traffic flow for all teaming modes. For outbound traffic, every packet is first classified into a flow, and then distributed to the selected physical adapter for transmission. The flow classification involves an efficient hash computation over known protocol fields. The resulting hash value is used to index into an Outbound Flow Hash Table.The selected Outbound Flow Hash Entry contains the index of the selected physical adapter responsible for transmitting this flow. The source MAC address of the packets will then be modified to the MAC address of the selected physical adapter. The modified packet is then passed to the selected physical adapter for transmission.

The outbound TCP and UDP packets are classified using Layer 3 and Layer 4 header information. This scheme improves the load distributions for popular Internet protocol services using well-known ports such as HTTP and FTP. Therefore, BASP performs load balancing on a TCP session basis and not on a packet-by-packet basis.

In the Outbound Flow Hash Entries, statistics counters are also updated after classification. The load-balancing engine uses these counters to periodically distribute the flows across teamed ports. The outbound code path has been designed to achieve best possible concurrency where multiple concurrent accesses to the Outbound Flow Hash Table are allowed.

For protocols other than TCP/IP, the first physical adapter will always be selected for outbound packets. The exception is Address Resolution Protocol (ARP), which is handled differently to achieve inbound load balancing.

## 4.4.3 Inbound Traffic Flow (SLB Only)

The Broadcom intermediate driver manages the inbound traffic flow for the SLB teaming mode. Unlike outbound load balancing, inbound load balancing can only be applied to IP addresses that are located in the same subnet as the load-balancing server. Inbound load balancing exploits a unique characteristic of Address Resolution Protocol (RFC0826), in which each IP host uses its own ARP cache to encapsulate the IP Datagram into an Ethernet frame. BASP carefully manipulates the ARP response to direct each IP host to send the inbound IP packet to the desired physical adapter. Therefore, inbound load balancing is a plan-ahead scheme based on statistical history of the inbound flows. New connections from a client to the server will always occur over the primary physical adapter (because the ARP Reply generated by the operating system protocol stack will always associate the logical IP address with the MAC address of the primary physical adapter).

Like the outbound case, there is an Inbound Flow Head Hash Table. Each entry inside this table has a singly linked list and each link (Inbound Flow Entries) represents an IP host located in the same subnet.

When an inbound IP Datagram arrives, the appropriate Inbound Flow Head Entry is located by hashing the source IP address of the IP Datagram. Two statistics counters stored in the selected entry are also updated. These counters are used in the same fashion as the outbound counters by the load-balancing engine periodically to reassign the flows to the physical adapter.

On the inbound code path, the Inbound Flow Head Hash Table is also designed to allow concurrent access. The link lists of Inbound Flow Entries are only referenced in the event of processing ARP packets and the periodic load balancing. There is no per packet reference to the Inbound Flow Entries. Even though the link lists are not bounded; the overhead in processing each non-ARP packet is always a constant. However, the processing of ARP packets, both inbound and outbound, depends on the number of links inside the corresponding link list.

On the inbound processing path, filtering is also employed to prevent broadcast packets from looping back through the system from other physical adapters.

## 4.4.4 Protocol Support

ARP and IP/TCP/UDP flows are load balanced. If the packet is an IP protocol only, such as ICMP or IGMP, then all data flowing to a particular IP address will go out through the same physical adapter. If the packet uses TCP or UDP for the L4 protocol, then the port number is added to the hashing algorithm, so two separate L4 flows can go out through two separate physical adapters to the same IP address.

For example, assume the client has an IP address of 10.0.0.1. All IGMP and ICMP traffic will go out the same physical adapter because only the IP address is used for the hash. The flow would look something like this:

```
IGMP ------> PhysAdapter1 ------> 10.0.0.1
ICMP ------> PhysAdapter1 ------> 10.0.0.1
```

If the server also sends a TCP and UDP flow to the same 10.0.0.1 address, they can be on the same physical adapter as IGMP and ICMP, or on completely different physical adapters from ICMP and IGMP. The stream may look like this:

```
IGMP ------> PhysAdapter1 ------> 10.0.0.1
ICMP ------> PhysAdapter1 ------> 10.0.0.1
TCP------> PhysAdapter1 ------> 10.0.0.1
UDP------> PhysAdatper1 ------> 10.0.0.1
```

Or the streams may look like this:

```
IGMP ------> PhysAdapter1 ------> 10.0.0.1
ICMP ------> PhysAdapter1 ------> 10.0.0.1
TCP------> PhysAdapter1 ------> 10.0.0.1
UDP------> PhysAdatper1 ------> 10.0.0.1
```

The actual assignment between adapters may change over time, but any protocol that is not TCP/UDP based goes over the same physical adapter because only the IP address is used in the hash.

### 4.4.5 Performance

Modern network interface cards provide many hardware features that reduce CPU utilization by offloading certain CPU intensive operations (→"4.7 Teaming and Other Advanced Networking Properties"(pg.138)). In contrast, the BASP intermediate driver is a purely software function that must examine every packet received from the protocol stacks and react to its contents before sending it out through a particular physical interface. Though the BASP driver can process each outgoing packet in near constant time, some applications that may already be CPU bound may suffer if operated over a teamed interface.In such cases, the application may be better suited to taking advantage of the failover capabilities of the intermediate driver, rather than the load balancing features. Or it may operate more efficiently over a single physical adapter that provides a particular hardware feature such as Large Send Offload.

## 4.5 Types of Teams

### 4.5.1 Switch-Independent

The Broadcom Smart Load Balancing type of team allows two to eight physical adapters to operate as a single virtual adapter. The greatest benefit of the SLB type of team is that it operates on any IEEE compliant switch and requires no special configuration.

#### Smart Load Balancing and Failover

SLB provides for switch-independent, bidirectional, fault-tolerant teaming and load balancing. Switch independence implies that there is no specific support for this function required in the switch, allowing SLB to be compatible with all switches. Under SLB, all adapters in the team have separate MAC addresses. The load-balancing algorithm operates on Layer 3 addresses of the source and destination nodes, which enables SLB to load balance both incoming and outgoing traffic.
The BASP intermediate driver continually monitors the physical ports in a team for link loss. In the event of link loss on any port, traffic is automatically diverted to other ports in the team. The SLB teaming mode supports switch fault tolerance by allowing teaming across different switches-provided the switches are on the same physical network or broadcast domain.

- **Network Communications**

  The following are the key attributes of SLB:
  - Failover mechanism - Link loss detection.
  - Load Balancing Algorithm - Inbound and outbound traffic are balanced through a Broadcom proprietary mechanism based on L4 flows.
  - Outbound Load Balancing using MAC Address - No
  - Outbound Load Balancing using IP Address - Yes
  - Multivendor Teaming - Supported (must include at least one Broadcom Ethernet adapter as a team member).

- **Applications**
  The SLB algorithm is most appropriate in home and small business environments where cost is a concern, or with commodity switching equipment. SLB teaming works with unmanaged Layer 2 switches and is a cost-effective way of getting redundancy and link aggregation at the server. Smart Load Balancing also supports teaming physical adapters with differing link capabilities. In addition, SLB is recommended when switch fault tolerance with teaming is required.
- **Configuration Recommendations**
  SLB supports connecting the teamed ports to hubs and switches if they are on the same broadcast domain. It does not support connecting to a router or Layer 3 switches because the ports must be on the same subnet.

## 4.5.2 Switch-Dependent

### Generic Static Trunking

This mode supports a variety of environments where the adapter link partners are statically configured to support a proprietary trunking mechanism. This mode could be used to support Lucent's Open Trunk, Cisco's Fast EtherChannel (FEC), and Cisco's Gigabit EtherChannel (GEC). In the static mode, as in generic link aggregation, the switch administrator needs to assign the ports to the team, and this assignment cannot be altered by the BASP, as there is no exchange of the Link Aggregation Control Protocol (LACP) frame.

With this mode, all adapters in the team are configured to receive packets for the same MAC address. Trunking operates on Layer 2 addresses and supports load balancing and failover for both inbound and outbound traffic. The BASP driver determines the load-balancing scheme for outbound packets, using Layer 4 protocols previously discussed, whereas the team link partner determines the load-balancing scheme for inbound packets.

The attached switch must support the appropriate trunking scheme for this mode of operation. Both the BASP and the switch continually monitor their ports for link loss. In the event of link loss on any port, traffic is automatically diverted to other ports in the team.

- **Network Communications**
  The following are the key attributes of Generic Static Trunking:
  - Failover mechanism - Link loss detection
  - Load Balancing Algorithm - Outbound traffic is balanced through Broadcom proprietary mechanism based L4 flows. Inbound traffic is balanced according to a switch specific mechanism.
  - Outbound Load Balancing using MAC Address - No
  - Outbound Load Balancing using IP Address - Yes
  - Multivendor Teaming - Supported (must include at least one Broadcom Ethernet adapter as a team member)
- **Applications**
  Generic trunking works with switches that support Cisco Fast EtherChannel, Cisco Gigabit EtherChannel, Extreme Networks Load Sharing and Bay Networks or IEEE 802.3ad Link Aggregation static mode. Since load balancing is implemented on Layer 2 addresses, all higher protocols such as IP, IPX, and NetBEUI are supported. Therefore, this is the recommended teaming mode when the switch supports generic trunking modes over SLB.

- **Configuration Recommendations**

  Static trunking supports connecting the teamed ports to switches if they are on the same broadcast domain and support generic trunking. It does not support connecting to a router or Layer 3 switches since the ports must be on the same subnet.

## Dynamic Trunking (IEEE 802.3ad Link Aggregation)

This mode supports link aggregation through static and dynamic configuration via the Link Aggregation Control Protocol (LACP). With this mode, all adapters in the team are configured to receive packets for the same MAC address. The MAC address of the first adapter in the team is used and cannot be substituted for a different MAC address. The BASP driver determines the load-balancing scheme for outbound packets, using Layer 4 protocols previously discussed, whereas the team's link partner determines the load-balancing scheme for inbound packets. Because the load balancing is implemented on Layer 2, all higher protocols such as IP, IPX, and NetBEUI are supported. The attached switch must support the 802.3ad Link Aggregation standard for this mode of operation. The switch manages the inbound traffic to the adapter while the BASP manages the outbound traffic. Both the BASP and the switch continually monitor their ports for link loss. In the event of link loss on any port, traffic is automatically diverted to other ports in the team.

- **Network Communications**

  The following are the key attributes of Dynamic Trunking:
  - Failover mechanism - Link loss detection
  - Load Balancing Algorithm - Outbound traffic is balanced through a Broadcom proprietary mechanism based on L4 flows. Inbound traffic is balanced according to a switch specific mechanism.
  - Outbound Load Balancing using MAC Address - No
  - Outbound Load Balancing using IP Address - Yes
  - Multivendor Teaming - Supported (must include at least one Broadcom Ethernet adapter as a team member)
- **Applications**

  Dynamic trunking works with switches that support IEEE 802.3ad Link Aggregation dynamic mode using LACP. Inbound load balancing is switch dependent. In general, the switch traffic is load balanced based on L2 addresses. In this case, all network protocols such as IP, IPX, and NetBEUI are load balanced. Therefore, this is the recommended teaming mode when the switch supports LACP, except when switch fault tolerance is required. SLB is the only teaming mode that supports switch fault tolerance.
- **Configuration Recommendations**

  Dynamic trunking supports connecting the teamed ports to switches as long as they are on the same broadcast domain and supports IEEE 802.3ad LACP trunking. It does not support connecting to a router or Layer 3 switches since the ports must be on the same subnet.

# 4.6 Attributes of the Features Associated with Each Type of Team

The attributes of the features associated with each type of team are summarized below.

- Smart Load Balancing™

| Feature | Attribute |
|---|---|
| User interface | Broadcom Advanced Control Suite 2 (BACS2) |
| Number of teams | Maximum 4 |
| Number of adapters per team | Maximum 8 |
| Hot replace | Yes |
| Hot add | Yes |
| Hot remove | Yes |
| Link speed support | Different speeds |
| Frame protocol | IP |
| Incoming packet management | BASP |
| Outgoing packet management | BASP |
| LiveLink support | Yes |
| Failover event | Loss of link |
| Failover time | <500 ms |
| Fallback time | 1.5 s(*1) (approximate) |
| MAC address | Different |
| Multivendor teaming | Yes |

*1: Make sure that Port Fast or Edge Port is enabled.

- Generic Trunking

| Feature | Attribute |
|---|---|
| User interface | Broadcom Advanced Control Suite 2 (BACS2) |
| Number of teams | Maximum 4 |
| Number of adapters per team | Maximum 8 |
| Hot replace | Yes |
| Hot add | Yes |
| Hot remove | Yes |
| Link speed support | Different speeds(*1) |
| Frame protocol | All |
| Incoming packet management | Switch |
| Outgoing packet management | BASP |
| Failover event | Loss of link only |
| Failover time | <500 ms |
| Fallback time | 1.5 s(*2) (approximate) |

| Feature | Attribute |
|---|---|
| MAC address | Same for all adapters |
| Multivendor teaming | Yes |

*1: Some switches require matching link speeds to correctly negotiate between trunk connections.

*2: Make sure that Port Fast or Edge Port is enabled.

• Dynamic Trunking

| Feature | Attribute |
|---|---|
| User interface | Broadcom Advanced Control Suite 2 (BACS2) |
| Number of teams | Maximum 4 |
| Number of adapters per team | Maximum 8 |
| Hot replace | Yes |
| Hot add | Yes |
| Hot remove | Yes |
| Link speed support | Different speeds |
| Frame protocol | All |
| Incoming packet management | Switch |
| Outgoing packet management | BASP |
| Failover event | Loss of link only |
| Failover time | <500 ms |
| Fallback time | 1.5 s(*1) (approximate) |
| MAC address | Same for all adapters |
| Multivendor teaming | Yes |

*1: Make sure that Port Fast or Edge Port is enabled.

## Speeds Supported for Each Type of Team

The various link speeds that are supported for each type of team are listed in "• Link Speeds in Teaming" (→pg.137). Mixed speed refers to the capability of teaming adapters that are running at different link speeds.

• Link Speeds in Teaming

| Type of Team | Link Speed | Traffic Direction | Speed Support |
|---|---|---|---|
| SLB | 10/100/1000 | Incoming/outgoing | Mixed speed |
| FEC | 100 | Incoming/outgoing | Same speed |
| GEC | 1000 | Incoming/outgoing | Same speed |
| IEEE 802.3ad | 10/100/1000 | Incoming/outgoing | Mixed speed |

E

# 4.7 Teaming and Other Advanced Networking Properties

Before creating a team, adding or removing team members, or changing advanced settings of a team member, make sure each team member has been configured in a similar way. Settings to check include VLANs and QoS Packet Tagging, Jumbo Frames, and the various offloads. Advanced adapter properties and teaming support are listed below.

- Advanced Adapter Properties and Teaming Support

| Adapter Properties | Supported by Teaming Virtual Adapter |
|---|---|
| Checksum Offload | Yes |
| IEEE 802.1p QoS Tagging | No |
| Large Send Offload | Yes (*1) |
| Jumbo Frames | Yes(*2) |
| IEEE 802.1Q VLANs | Yes(*3) |
| Wake on LAN | No |
| Preboot Execution environment (PXE) | Yes(*4) |

*1: All adapters on the team must support this feature. Some adapters may not support this feature if ASF/IPMI is also enabled.

*2: Must be supported by all adapters in the team.

*3: Only for Broadcom adapters.

*4: As a PXE server only, not as a client.

A team does not necessarily inherit adapter properties. Instead, various properties depend on the specific capability. For instance, an example would be flow control, which is a physical adapter property and has nothing to do with BASP, and will be enabled on a particular adapter if the miniport driver for that adapter has flow control enabled.

**POINT**

- All adapters on the team must support the property listed in "• Advanced Adapter Properties and Teaming Support" (→pg.138) in order for the team to support the property.

## Checksum Offload

Checksum Offload is a property of the Broadcom network adapters that allows the TCP/IP/UDP checksums for send and receive traffic to be calculated by the adapter hardware rather than by the host CPU. In high-traffic situations, this can allow a system to handle more connections more efficiently than if the host CPU were forced to calculate the checksums. This property is inherently a hardware property and would not benefit from a software-only implementation. An adapter that supports Checksum Offload advertises this capability to the operating system so that the checksum does not need to be calculated in the protocol stack. Checksum Offload is only supported for IPv4 at this time.

## IEEE 802.1p QoS Tagging

The IEEE 802.1p standard includes a 3-bit field (supporting a maximum of 8 priority levels), which allows for traffic prioritization. The BASP intermediate driver does not support IEEE 802.1p QoS tagging.

## Large Send Offload

Large Send Offload (LSO) is a feature provided by Broadcom network adapters that prevents an upper level protocol such as TCP from breaking a large data packet into a series of smaller packets with headers appended to them. The protocol stack need only generate a single header for a data packet as large as 64 KB, and the adapter hardware breaks the data buffer into appropriately-sized Ethernet frames with the correctly sequenced header (based on the single header originally provided).

## Jumbo Frames

The use of jumbo frames was originally proposed by Alteon Networks, Inc. in 1998 and increased the maximum size of an Ethernet frame to a maximum size of 9000 bytes. Though never formally adopted by the IEEE 802.3 Working Group, support for jumbo frames has been implemented in this product. The BASP intermediate driver supports jumbo frames, provided that all of the physical adapters in the team also support jumbo frames and the same size is set on all adapters in the team.

## IEEE 802.1Q VLANs

In 1998, the IEEE approved the 802.3ac standard, which defines frame format extensions to support Virtual Bridged Local Area Network tagging on Ethernet networks as specified in the IEEE 802.1Q specification. The VLAN protocol permits insertion of a tag into an Ethernet frame to identify the VLAN to which a frame belongs. If present, the 4-byte VLAN tag is inserted into the Ethernet frame between the source MAC address and the length/type field. The first 2-bytes of the VLAN tag consist of the IEEE 802.1Q tag type, whereas the second 2 bytes include a user priority field and the VLAN identifier (VID). Virtual LANs (VLANs) allow the user to split the physical LAN into logical subparts. Each defined VLAN behaves as its own separate network, with its traffic and broadcasts isolated from the others, thus increasing bandwidth efficiency within each logical group. VLANs also enable the administrator to enforce appropriate security and quality of service (QoS) policies. The BASP supports the creation of 64 VLANs per team or adapter: 63 tagged and 1 untagged. The operating system and system resources, however, limit the actual number of VLANs. VLAN support is provided according to IEEE 802.1Q and is supported in a teaming environment as well as on a single adapter. Note that VLANs are supported only with homogeneous teaming and not in a multivendor teaming environment. The BASP intermediate driver supports VLAN tagging. One or more VLANs may be bound to a single instance of the intermediate driver.

### Preboot Execution Environment

The Preboot Execution Environment (PXE) allows a system to boot from an operating system image over the network. By definition, PXE is invoked before an operating system is loaded, so there is no opportunity for the BASP intermediate driver to load and enable a team. As a result, teaming is not supported as a PXE client, though a physical adapter that participates in a team when the operating system is loaded may be used as a PXE client. Whereas a teamed adapter cannot be used as a PXE client, it can be used for a PXE server, which provides operating system images to PXE clients using a combination of Dynamic Host Control Protocol (DHCP) and the Trivial File Transfer Protocol (TFTP). Both of these protocols operate over IP and are supported by all teaming modes.

# 4.8 General Network Considerations

## 4.8.1 Teaming Across Switches

SLB teaming can be configured across switches. The switches, however, must be connected together. Generic Trunking and Link Aggregation do not work across switches because each of these implementations requires that all physical adapters in a team share the same Ethernet MAC address. It is important to note that SLB can only detect the loss of link between the ports in the team and their immediate link partner. SLB has no way of reacting to other hardware failures in the switches and cannot detect loss of link on other ports.

## 4.8.2 Switch-Link Fault Tolerance

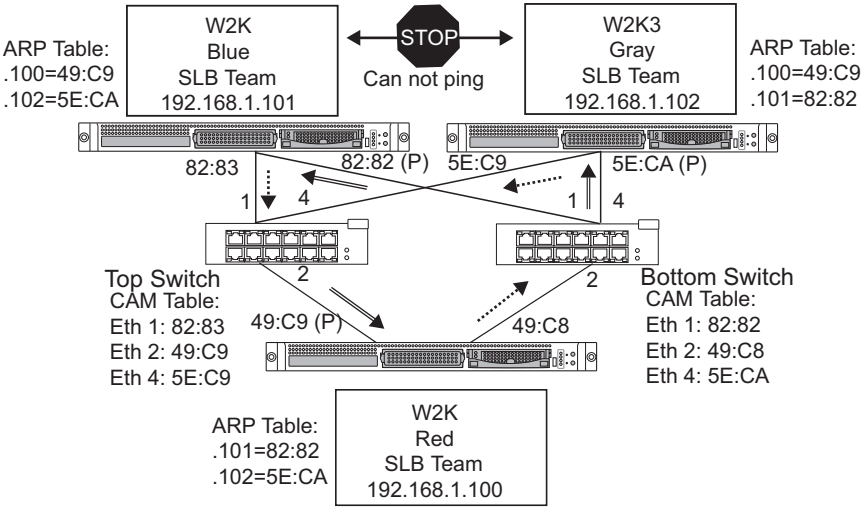
The diagrams below describe the operation of an SLB team in a switch fault tolerant configuration. We show the mapping of the ping request and ping replies in an SLB team with two active members. All servers (Blue, Gray and Red) have a continuous ping to each other. "• Teaming Across Switches Without an Interswitch Link" (→pg.141) is a setup without the interconnect cable in place between the two switches. "• Teaming Across Switches With Interconnect" (→pg.142) has the interconnect cable in place, and "• Failover Event" (→pg.142) is an example of a failover event with the Interconnect cable in place. These scenarios describe the behavior of teaming across the two switches and the importance of the interconnect link.

The diagrams show the secondary team member sending the ICMP echo requests (arrow of a dotted line), while the primary team member receives the respective ICMP echo replies (arrow of a double line). This illustrates a key characteristic of the teaming software. The load balancing algorithms do not synchronize how frames are load balanced when sent or received. In other words, frames for a given conversation can go out and be received on different interfaces in the team. This is true for all types of teaming supported by Broadcom. Therefore, an interconnect link must be provided between the switches that connect to ports in the same team.

In the configuration without the interconnect, an ICMP Request from Blue to Gray goes out port 82:83 destined for Gray port 5E:CA, but the Top Switch has no way to send it there because it cannot go along the 5E:C9 port on Gray. A similar scenario occurs when Gray attempts to ping Blue. An ICMP Request goes out on 5E:C9 destined for Blue 82:82, but cannot get there. Top Switch does not have an entry for 82:82 in its CAM table because there is no interconnect between the two switches. Pings, however, flow between Red and Blue and between Red and Gray.

Furthermore, a failover event would cause additional loss of connectivity. Consider a cable disconnect on the Top Switch port 4. In this case, Gray would send the ICMP Request to Red 49:C9, but because the Bottom switch has no entry for 49:C9 in its CAM Table, the frame is flooded to all its ports but cannot find a way to get to 49:C9.

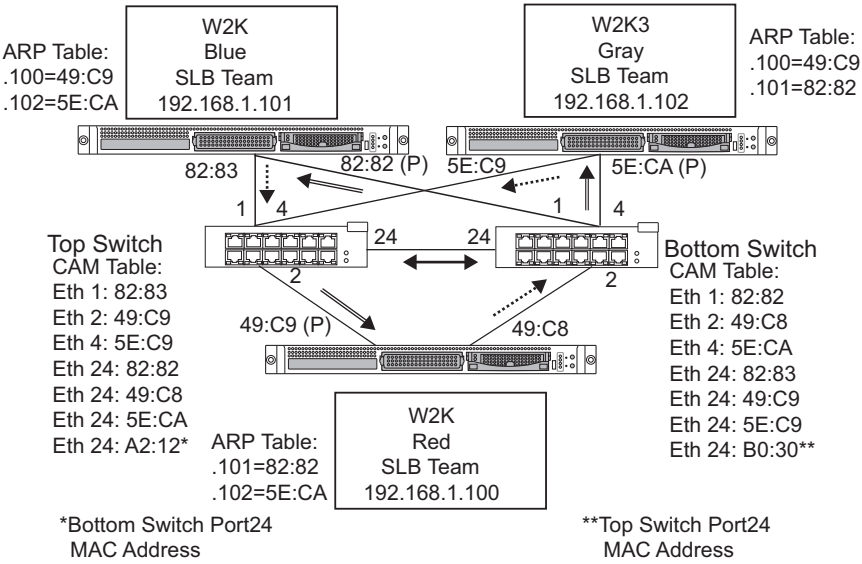
- Teaming Across Switches Without an Interswitch Link




The addition of a link between the switches allows traffic from/to Blue and Gray to reach each other without any problems. Note the additional entries in the CAM table for both switches. The link interconnect is critical for the proper operation of the team. As a result, it is highly advisable to have a link aggregation trunk to interconnect the two switches to ensure high availability for the connection.

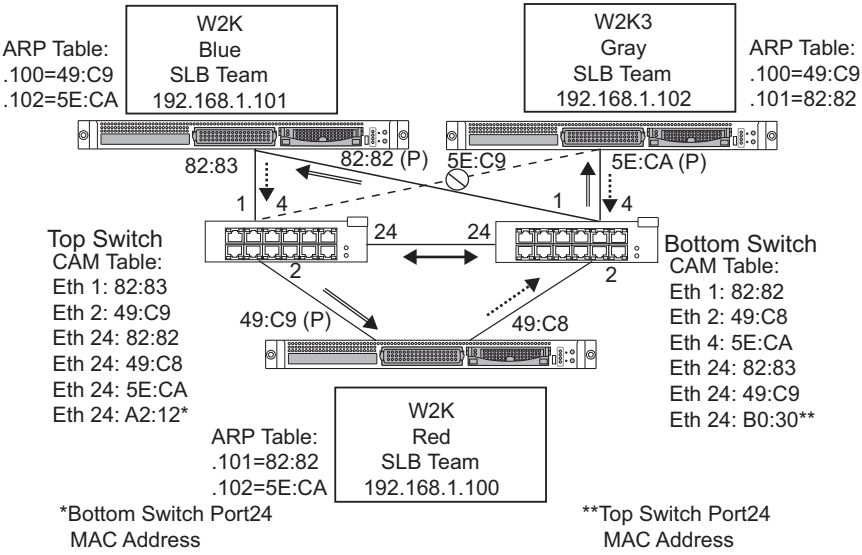
E

• Teaming Across Switches With Interconnect




"• Teaming Across Switches With Interconnect" (→pg.142) represents a failover event in which the cable is unplugged on the Top Switch port 4. This is a successful failover with all stations pinging each other without loss of connectivity.

• Failover Event



## 4.8.3 Spanning Tree Algorithm

In Ethernet networks, only one active path may exist between any two bridges or switches. Multiple active paths between switches can cause loops in the network. When loops occur, some switches recognize stations on both sides of the switch. This situation causes the forwarding algorithm to malfunction allowing duplicate frames to be forwarded. Spanning tree algorithms provide path redundancy by defining a tree that spans all of the switches in an extended network and then forces certain redundant data paths into a standby (blocked) state. At regular intervals, the switches in the network send and receive spanning tree packets that they use to identify the path. If one network segment becomes unreachable, or if spanning tree costs change, the spanning tree algorithm reconfigures the spanning tree topology and re-establishes the link by activating the standby path. Spanning tree operation is transparent to end stations, which do not detect whether they are connected to a single LAN segment or a switched LAN of multiple segments.
Spanning Tree Protocol (STP) is a Layer 2 protocol designed to run on bridges and switches. The specification for STP is defined in IEEE 802.1d. The main purpose of STP is to ensure that you do not run into a loop situation when you have redundant paths in your network. STP detects/disables network loops and provides backup links between switches or bridges. It allows the device to interact with other STP compliant devices in your network to ensure that only one path exists between any two stations on the network.

After a stable network topology has been established, all bridges listen for hello BPDUs (Bridge Protocol Data Units) transmitted from the root bridge. If a bridge does not get a hello BPDU after a predefined interval (Max Age), the bridge assumes that the link to the root bridge is down. This bridge then initiates negotiations with other bridges to reconfigure the network to re-establish a valid network topology. The process to create a new topology can take up to 50 seconds. During this time, end-to-end communications are interrupted.

The use of Spanning Tree is not recommended for ports that are connected to end stations, because by definition, an end station does not create a loop within an Ethernet segment. Additionally, when a teamed adapter is connected to a port with Spanning Tree enabled, users may experience unexpected connectivity problems. For example, consider a teamed adapter that has a lost link on one of its physical adapters. If the physical adapter were to be reconnected (also known as fallback), the intermediate driver would detect that the link has been reestablished and would begin to pass traffic through the port. Traffic would be lost if the port was temporarily blocked by the Spanning Tree Protocol.

## 4.8.4 Topology Change Notice (TCN)

A bridge/switch creates a forwarding table of MAC addresses and port numbers by learning the source MAC address that received on a particular port. The table is used to forward frames to a specific port rather than flooding the frame to all ports. The typical maximum aging time of entries in the table is 5 minutes. Only when a host has been silent for 5 minutes would its entry be removed from the table. It is sometimes beneficial to reduce the aging time. For example, when a forwarding link goes to blocking and a different link goes from blocking to forwarding. This change could take up to 50 seconds. At the end of the STP re-calculation a new path would be available for communications between end stations. However, because the forwarding table would still have entries based on the old topology, communications may not be reestablished until after 5 minutes when the affected ports entries are removed from the table. Traffic would then be flooded to all ports and re-learned. In this case it is beneficial to reduce the aging time. This is the purpose of a topology change notice (TCN) BPDU. The TCN is sent from the affected bridge/switch to the root bridge/switch. As soon as a bridge/switch detects a topology change (a link going down or a port going to forwarding) it sends a TCN to the root bridge via its root port. The root bridge then advertises a BPDU with a Topology Change to the entire network.This causes every bridge to reduce the MAC table aging time to 15 seconds for a specified amount of time. This allows the switch to re-learn the MAC addresses as soon as STP re-converges.

Topology Change Notice BPDUs are sent when a port that was forwarding changes to blocking or transitions to forwarding. A TCN BPDU does not initiate an STP recalculation. It only affects the aging time of the forwarding table entries in the switch.It will not change the topology of the network or create loops. End nodes such as servers or clients trigger a topology change when they power off and then power back on.

### 4.8.5 Port Fast/Edge Port

To reduce the effect of TCNs on the network (for example, increasing flooding on switch ports), end nodes that are powered on/off often should use the Port Fast or Edge Port setting on the switch port they are attached to. Port Fast or Edge Port is a command that is applied to specific ports and has the following effects:

- Ports coming from link down to link up will be put in the forwarding STP mode instead of going from listening to learning and then to forwarding. STP is still running on these ports.
- The switch does not generate a Topology Change Notice when the port is going up or down.

### 4.8.6 Layer 3 Routing/Switching

The switch that the teamed ports are connected to must not be a Layer 3 switch or router. The ports in the team must be in the same network.

### 4.8.7 Teaming with Hubs (for troubleshooting purposes only)

SLB teaming can be used with 10/100 hubs, but it is only recommended for troubleshooting purposes, such as connecting a network analyzer in the event that switch port mirroring is not an option.

### 4.8.8 Hub Usage in Teaming Network Configurations

Although the use of hubs in network topologies is functional in some situations, it is important to consider the throughput ramifications when doing so. Network hubs have a maximum of 100 Mbps half-duplex link speed, which severely degrades performance in either a Gigabit or 100 Mbps switched-network configuration. Hub bandwidth is shared among all connected devices; as a result, when more devices are connected to the hub, the bandwidth available to any single device connected to the hub is reduced in direct proportion to the number of devices connected to the hub.

It is not recommended to connect team members to hubs; only switches should be used to connect to teamed ports. An SLB team, however, can be connected directly to a hub for troubleshooting purposes. Other team types can result in a loss of connectivity if specific failures occur and should not be used with hubs.

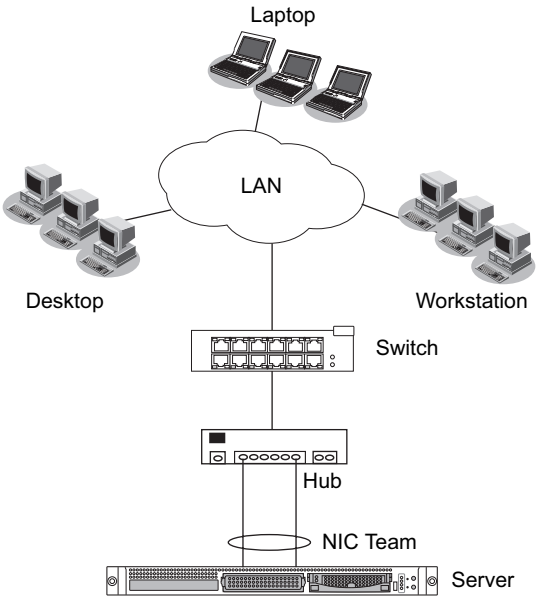
## 4.8.9 SLB Teams

SLB teams are the only teaming type not dependant on switch configuration. The server intermediate driver handles the load balancing and fault tolerance mechanisms with no assistance from the switch. These elements of SLB make it the only team type that maintains failover and fallback characteristics when team ports are connected directly to a hub.

### SLB Team Connected to a Single Hub

SLB teams configured as shown in "• Team Connected to a Single Hub" (→pg.146) maintain their fault tolerance properties. Either server connection could potentially fail, and network functionality is maintained. Clients could be connected directly to the hub, and fault tolerance would still be maintained; server performance, however, would be degraded.

• Team Connected to a Single Hub




### Generic and Dynamic Trunking (FEC/GEC/IEEE 802.3ad)

FEC/GEC and IEEE 802.3ad teams cannot be connected to any hub configuration. These team types must be connected to a switch that has also been configured for this team type.

### Teaming with Microsoft NLB/WLBS

It is known that the SLB mode of teaming does not work in an NLB unicast environment. It is not known, however, why the SLB mode should not work in a NLB multicast environment. The SLB teaming algorithm is mutually exclusive with the NLB unicast mechanism.

## 4.8.10 Troubleshooting Teaming Problems

When running a protocol analyzer over a virtual adapter teamed interface, the MAC address shown in the transmitted frames may not be correct. The analyzer does not show the frames as constructed by BASP and shows the MAC address of the team and not the MAC address of the interface transmitting the frame. It is suggested to use the following process to monitor a team:

- Mirror all uplink ports from the team at the switch.
- If the team spans two switches, mirror the interlink trunk as well.
- Sample all mirror ports independently.
- On the analyzer, use an adapter and driver that does not filter QoS and VLAN information.

### Teaming Configuration Tips

When troubleshooting network connectivity or teaming functionality issues, ensure that the following information is true for your configuration.

- Although mixed-speed SLB teaming is supported, it is recommended that all adapters in a team be the same speed (either all Gigabit Ethernet or all Fast Ethernet).
- If LiveLink is not enabled, disable Spanning Tree Protocol or enable an STP mode that bypasses the initial phases (for example, Port Fast, Edge Port) for the switch ports connected to a team.
- All switches that the team is directly connected to must have the same hardware revision, firmware revision, and software revision to be supported.
- To be teamed, adapters should be members of the same VLAN. In the event that multiple teams are configured, each team should be on a separate network.
- Do not use the Locally Administered Address on any physical adapter that is a member of a team.
- Remove any static IP address from the individual physical team members before the team is built.
- A team that requires maximum throughput should use LACP or GEC\FEC. In these cases, the intermediate driver is only responsible for the outbound load balancing while the switch performs the inbound load balancing.
- Aggregated teams (802.3ad \ LACP and GEC\FEC) must be connected to only a single switch that supports IEEE 802.3a, LACP or GEC/FEC.
- It is not recommended to connect any team to a hub, as a hub only support half duplex. Hubs should be connected to a team for troubleshooting purposes only.
- Verify the base (Miniport) and team (intermediate) drivers are from the same release package. The mixing of base and teaming drivers from different CD releases is not supported.
- Test the connectivity to each physical adapter prior to teaming.
- Test the failover and fallback behavior of the team before placing into a production environment.
- When moving from a nonproduction network to a production network, it is strongly recommended to test again for failover and fallback.
- Test the performance behavior of the team before placing into a production environment.

## Troubleshooting Guidelines

Before you call for support, make sure you have completed the following steps for troubleshooting network connectivity problems when the server is using adapter teaming.

- Make sure the link light is ON for every adapter and all the cables are attached.
- Check that the matching base and intermediate drivers belong to the same release and are loaded correctly.
- Check for a valid IP Address using the Windows ipconfig command.
- Check that STP is disabled or Edge Port/Port Fast is enabled on the switch ports connected to the team or that LiveLink is being used.
- Check that the adapters and the switch are configured identically for link speed and duplex.
- If possible, break the team and check for connectivity to each adapter independently to confirm that the problem is directly associated with teaming.
- Check that all switch ports connected to the team are on the same VLAN.
- Check that the switch ports are configured properly for Generic Trunking (FEC/GEC)/802.3ad-Draft Static type of teaming and that it matches the adapter teaming type. If the system is configured for an SLB type of team, make sure the corresponding switch ports are not configured for Generic Trunking (FEC/GEC)/802.3ad-Draft Static types of teams.

## Frequently Asked Questions

| Question | Answer |
|---|---|
| Under what circumstances is traffic not load balanced? Why is all traffic not load balanced evenly across the team members? | The bulk of traffic does not use IP/TCP/UDP or the bulk of the clients are in a different network. The receive load balancing is not a function of traffic load, but a function of the number of clients that are connected to the server. |
| What network protocols are load balanced when in a team? | Broadcom's teaming software only supports IP/TCP/UDP traffic. All other traffic is forwarded to the primary adapter. |
| Which protocols are load balanced with SLB and which ones are not? | Only IP/TCP/UDP protocols are load balanced in both directions: send and receive. IPX is load balanced on the transmit traffic only. |
| Can I team a port running at 100 Mbps with a port running at 1000 Mbps? | Mixing link speeds within a team is only supported for Smart Load Balancing™ teams and 802.3ad teams. |
| Can I team a fiber adapter with a copper Gigabit Ethernet adapter? | Yes with SLB, and yes if the switch allows for it in FEC/GEC and 802.3ad. |
| What is the difference between adapter load balancing and Microsoft's Network Load Balancing (NLB)? | Adapter load balancing is done at a network session level, whereas NLB is done at the server application level. |

| Question | Answer |
|---|---|
| Can I connect the teamed adapters to a hub? | Teamed ports can be connected to a hub for troubleshooting purposes only. However, this practice is not recommended for normal operation because the performance would be degraded due to hub limitations. Connect the teamed ports to a switch instead. |
| Can I connect the teamed adapters to ports in a router? | No. All ports in a team must be on the same network; in a router, however, each port is a separate network by definition. All teaming modes require that the link partner be a Layer 2 switch. |
| Can I use teaming with Microsoft Cluster Services? | Yes. Teaming is supported on the public network only, not on the private network used for the heartbeat link. |
| Can PXE work over a virtual adapter (team)? | A PXE client operates in an environment before the operating system is loaded; as a result, virtual adapters have not been enabled yet. If the physical adapter supports PXE, then it can be used as a PXE client, whether or not it is part of a virtual adapter when the operating system loads. PXE servers may operate over a virtual adapter. |
| What is the maximum number of ports that can be teamed together? | Up to eight ports can be assigned to a team. |
| What is the maximum number of teams that can be configured on the same server? | Up to four teams can be configured on the same server. |
| Why does my team loose connectivity for the first 30 to 50 seconds after the Primary adapter is restored (fallback)? | Answer: Because Spanning Tree Protocol is bringing the port from blocking to forwarding. You must enable Port Fast or Edge Port on the switch ports connected to the team or use LiveLink to account for the STP delay. |
| Can I connect a team across multiple switches? | Smart Load Balancing can be used with multiple switches because each physical adapter in the system uses a unique Ethernet MAC address. Link Aggregation and Generic Trunking cannot operate across switches because they require all physical adapters to share the same Ethernet MAC address. |
| How do I upgrade the intermediate driver (BASP)? | The intermediate driver cannot be upgraded through the Local Area Connection Properties. It must be upgraded using the Setup installer. |

| Question | Answer |
|---|---|
| Can I configure NLB and teaming concurrently? | Yes, but only when running NLB in a multicast mode (NLB is not supported with MS Cluster Services). |
| Should both the backup server and client servers that are backed up be teamed? | Because the backup server is under the most data load, it should always be teamed for link aggregation and failover. A fully redundant network, however, requires that both the switches and the backup clients be teamed for fault tolerance and link aggregation. |
| Is there any special configuration required in the tape backup software or hardware to work with adapter teaming? | No special configuration is required in the tape software to work with teaming. Teaming is transparent to tape backup applications. |
| How do I know what driver I am currently using? | In all operating systems, the most accurate method for checking the driver revision is to physically locate the driver file and check the properties. |
| Can SLB detect a switch failure in a Switch Fault Tolerance configuration? | No. SLB can only detect the loss of link between the teamed port and its immediate link partner. SLB cannot detect link failures on other ports. |
| Why does my team lose connectivity for the first 30 to 50 seconds after the primary adapter is restored (fall-back after a failover)? | During a fall-back event, link is restored causing Spanning Tree Protocol to configure the port for blocking until it determines that it can move to the forwarding state. You must enable Port Fast or Edge Port on the switch ports connected to the team to prevent the loss of communications caused by STP. |
| Where do I monitor real time statistics for an adapter team in a Windows server? | Use the BACS2 to monitor general, IEEE 802.3 and custom counters. |

# 4.9 Event Log Messages

## 4.9.1 Windows System Event Log messages

The known base and intermediate Windows System Event Log status messages for this product are listed in "4.9.2 Base Driver (Physical Adapter/Miniport)" (→pg.151) and "4.9.3 Intermediate Driver (Virtual Adapter/Team)" (→pg.153). As a Broadcom adapter driver loads, Windows places a status code in the system event viewer. There may be up to two classes of entries for these event codes depending on whether both drivers are loaded (one set for the base or miniport driver and one set for the intermediate or teaming driver).

## 4.9.2 Base Driver (Physical Adapter/Miniport)

"• Base Driver Event Log Messages" (→pg.151) lists the event log messages supported by the base driver, explains the cause for the message, and provides the recommended action.

• Base Driver Event Log Messages

| Message Number | Message | Cause | Corrective Action |
|---|---|---|---|
| 1 | Failed to allocate memory for the device block. Check system memory resource usage. | The driver cannot allocate memory from the operating system. | Close running applications to free memory. |
| 2 | Failed to allocate map registers. | The driver cannot allocate map registers from the operating system. | Unload other drivers that may allocate map registers. |
| 3 | Failed to access configuration information. Reinstall the network driver. | The driver cannot access PCI configuration space registers on the adapter. | For add-in adapters: reseat the adapter in the slot, move the adapter to another PCI slot, or replace the adapter. |
| 4 | The network link is down. Check to make sure the network cable is properly connected. | The adapter has lost its connection with its link partner. | Check that the network cable is connected, verify that the network cable is the right type, and verify that the link partner (for example, switch or hub) is working correctly. |
| 5 | The network link is up. | The adapter has established a link. | Informational message only. No action is required. |
| 6 | Network controller configured for 10Mb half-duplex link. | The adapter has been manually configured for the selected line speed and duplex settings. | Informational message only. No action is required. |

E

| Message Number | Message | Cause | Corrective Action |
|---|---|---|---|
| 7 | Network controller configured for 10Mb full-duplex link. | The adapter has been manually configured for the selected line speed and duplex settings. | Informational message only.<br>No action is required. |
| 8 | Network controller configured for 100Mb half-duplex link. | The adapter has been manually configured for the selected line speed and duplex settings. | Informational message only.<br>No action is required. |
| 9 | Network controller configured for 100Mb full-duplex link. | The adapter has been manually configured for the selected line speed and duplex settings. | Informational message only.<br>No action is required. |
| 10 | Network controller configured for 1Gb half-duplex link. | The adapter has been manually configured for the selected line speed and duplex settings. | Informational message only.<br>No action is required. |
| 11 | Network controller configured for 1Gb full-duplex link. | The adapter has been manually configured for the selected line speed and duplex settings. | Informational message only.<br>No action is required. |
| 12 | Medium not supported. | The operating system does not support the IEEE 802.3 medium. | Reboot the operating system, run a virus check, run a disk check (chkdsk), and reinstall the operating system. |
| 13 | Unable to register the interrupt service routine. | The device driver cannot install the interrupt handler. | Reboot the operating system; remove other device drivers that may be sharing the same IRQ. |
| 14 | Unable to map IO space. | The device driver cannot allocate memory-mapped I/O to access driver registers. | Remove other adapters from the system, reduce the amount of physical memory installed, and replace the adapter. |
| 15 | Driver initialized successfully. | The driver has successfully loaded. | Informational message only.<br>No action is required. |
| 16 | NDIS is resetting the miniport driver. | The NDIS layer has detected a problem sending/receiving packets and is resetting the driver to resolve the problem. | Run BACS2 diagnostics; check that the network cable is good. |

| Message Number | Message | Cause | Corrective Action |
|---|---|---|---|
| 17 | Unknown PHY detected. Using a default PHY initialization routine. | The driver could not read the PHY ID. | Replace the adapter. |
| 18 | This driver does not support this device. Upgrade to the latest driver. | The driver does not recognize the installed adapter. | Upgrade to a driver version that supports this adapter. |
| 19 | Driver initialization failed. | Unspecified failure during driver initialization. | Reinstall the driver, update to a newer driver, run BACS2 diagnostics, or replace the adapter. |

### 4.9.3 Intermediate Driver (Virtual Adapter/Team)

The intermediate driver is identified by BLFM regardless of the base driver revision. "• Intermediate Driver Event Log Messages" (→pg.153) lists the event log messages supported by the intermediate driver, explains the cause for the message, and provides the recommended action.

• Intermediate Driver Event Log Messages

| Message Number | Message | Cause | Corrective Action |
|---|---|---|---|
| 1 | Unable to register with NDIS. | The driver cannot register with the NDIS interface. | Unload any NDIS drivers. |
| 2 | Unable to instantiate the management interface. | The driver cannot create a device instance. | Reboot the operating system. |
| 3 | Unable to create symbolic link for the management interface. | Another driver has created a conflicting device name. | Unload the conflicting device driver that uses the name "Blf". |
| 4 | Broadcom Advanced Server Program Driver has started. | The driver has started. | Informational message only.<br>No action is required. |
| 5 | Broadcom Advanced Server Program Driver has stopped. | The driver has stopped. | Informational message only.<br>No action is required. |
| 6 | Could not allocate memory for internal data structures. | The driver cannot allocate memory from the operating system. | Close running applications to free memory. |

| Message Number | Message | Cause | Corrective Action |
|---|---|---|---|
| 7 | Could not bind to adapter. | The driver could not open one of the team physical adapters. | Unload and reload the physical adapter driver, install an updated physical adapter driver, or replace the physical adapter. |
| 8 | Successfully bind to adapter. | The driver successfully opened the physical adapter. | Informational message only.<br>No action is required. |
| 9 | Network adapter is disconnected. | The physical adapter is not connected to the network (it has not established link). | Check that the network cable is connected, verify that the network cable is the right type, and verify that the link partner (switch or hub) is working correctly. |
| 10 | Network adapter is connected. | The physical adapter is connected to the network (it has established link). | Informational message only.<br>No action is required. |
| 11 | Broadcom Advanced Program Features Driver is not designed to run on this version of Operating System. | The driver does not support the operating system on which it is installed. | Consult the driver release notes and install the driver on a supported operating system or update the driver. |
| 12 | Hot-standby adapter is selected as the primary adapter for a team without a load balancing adapter. | A standby adapter has been activated. | Replace the failed physical adapter. |
| 13 | Network adapter does not support Advanced Failover. | The physical adapter does not support the Broadcom NIC Extension (NICE). | Replace the adapter with one that does support NICE. |
| 14 | Network adapter is enabled via management interface. | The driver has successfully enabled a physical adapter through the management interface. | Informational message only.<br>No action is required. |

| Message Number | Message | Cause | Corrective Action |
|---|---|---|---|
| 15 | Network adapter is disabled via management interface. | The driver has successfully disabled a physical adapter through the management interface. | Informational message only.<br>No action is required. |
| 16 | Network adapter is activated and is participating in network traffic. | A physical adapter has been added to or activated in a team. | Informational message only.<br>No action is required. |
| 17 | Network adapter is de-activated and is no longer participating in network traffic. | The driver does not recognize the installed adapter. | Informational message only.<br>No action is required. |

# 5 Broadcom Advanced Control Suite 2 (BACS2)

This chapter explains the Broadcom Advanced Control Suite 2 (BACS2).

## 5.1 BACS2 Overview

BACS2 is an integrated utility that provides useful information about each network adapter that is installed in your system. BACS2 also enables you to perform detailed tests, diagnostics, and analyses on each adapter, as well as to view and modify property values and view traffic statistics for each adapter.
BACS2 contains three panes:

- In the Information/Task pane, users can view available information and perform certain tests, diagnostics, and analysis on a selected device by clicking a specific tab.
- To the left of the Information/Task pane is the Device Name pane, which lists the names of the individual network adapters and the individual members of teams that have been created.
- A third pane contains the Menu bar.

Broadcom Advanced Server Program (BASP), which runs within Broadcom Advanced Control Suite 2 (BACS2), is used in Expert Mode to configure teams for load balancing, fault tolerance, and virtual local area networks (VLANs). The Teaming Wizard can also be used to configure teams and VLANs. BASP functionality is available only on systems that use at least one network adapter.

IMPORTANT

- Link aggregation is not supported in the Blade Server.

## 5.1.1 Types of Information Provided by BACS2

BACS2 lists all of the network adapters in your system and provides the following information (if available) about each adapter:

- Driver Status
- MAC Address
- Link Status
- IP Address
- Memory Address
- Physical Address
- Speed
- Duplex
- Slot No.
- Driver Name
- Driver Version
- Driver Date
- Firmware Version
- ASIC Version
- Bus Type
- Bus No.
- Device No.
- Function No.
- Interrupt Request
- Team Name
- Team Type
- VLAN Name
- VLAN ID
- Properties

The details of a function provided by BACS2 are shown below.

| Function | Details |
|---|---|
| Vital Sign | At-a-glance information on all of the LAN adapters in your system.<br>→"5.4.1 Vital Sign"(pg.162) |
| Resources | Shows the resource settings for the selected adapter.<br>→"5.4.2 Resources"(pg.165) |
| Hardware | Shows the hardware information for the selected adapter.<br>→"5.4.3 Hardware"(pg.166) |
| Advanced | Shows the available properties and their values for the selected adapter.<br>→"5.4.4 Advanced"(pg.167) |
| Network Test | Confirms network connectivity to a remote station.<br>→"5.4.5 Network Test"(pg.170) |
| Diagnostics | Performs comprehensive diagnostics.<br>→"5.4.6 Diagnostics"(pg.170) |
| Statistics | Provides detailed performance statistics for the selected adapter.<br>→"5.4.7 Statistics"(pg.172) |
| Resource Allocations | Displays a pie chart of the allocated TOE, iSCSI, and RDMA connections, as well as the unallocated and unlicensed resources. Only available with this product.<br>**POINT**<br>▸ This setting is not supported. |
| Licenses | Displays licensing information for the TOE, iSCSI, and RDMA technologies. Only available with this product.<br>→"5.4.8 Licenses"(pg.175) |

E

# 5.2 Installing the BACS2

If [Broadcom Control Suite 2] is not displayed in the "Control Panel", install BACS2 according to the following installation procedures:

**POINT**

- Ensure that this product is installed in the Server Blade before installing BACS2.
- Before you begin the installation, close all applications, windows, or dialog boxes.
- To use TCP/IP Offload Engine (TOE), you must have Windows Server 2003 with Scalable Networking Pack (SNP)

**IMPORTANT**

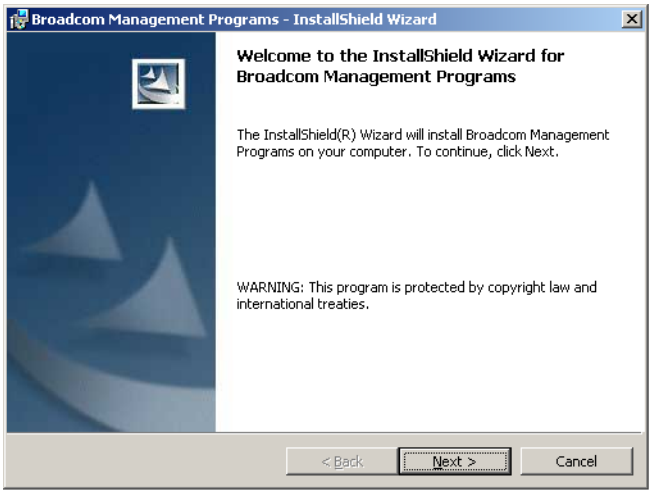
- The installer checks if SNP for Windows Server 2003 is installed on the machine.
  If it is installed, the installer installs the NDIS 5.2 driver, which is necessary in order to use TOE. If SNP for Windows Server 2003 is not installed on the machine,
  the installer will install the NDIS 5.1 driver, a user cannot use TOE.
- Get the Broadcom Control Suite from the ServerStart CD-ROM included with the BX620 S4 server blade and install.
  If using Broadcom, refer to the operation manual or help file included with the driver.

## For Windows Server 2003 x64

### 1 Start the following EXE file from the ServerStart Disc1 CD-ROM attached to the BX620 S4.

[CD-ROM drive]: \PROGRAMS\GENERAL\Broadcom\MgmtApps_x64\setup.exe

The installer starts up.


Broadcom Management Programs - InstallShield Wizard
Welcome to the InstallShield Wizard for Broadcom Management Programs
The InstallShield(R) Wizard will install Broadcom Management Programs on your computer. To continue, click Next.
WARNING: This program is protected by copyright law and international treaties.
< Back
Next >
Cancel

### 2 Click [Next].

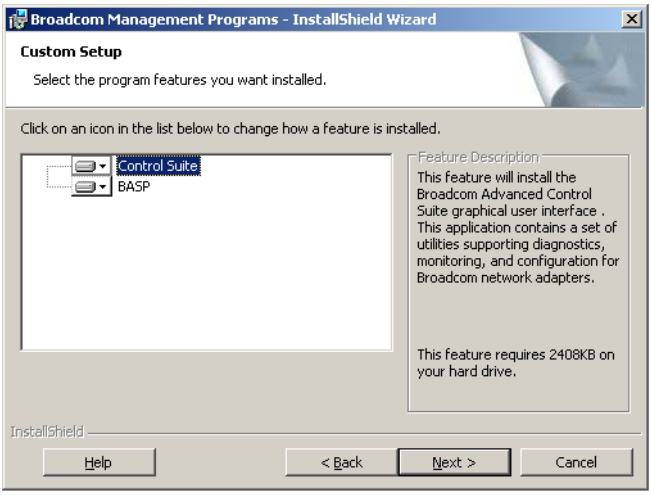
License agreement window appears

Broadcom Management Programs - InstallShield Wizard
License Agreement
Please read the following license agreement carefully.
LICENSE AGREEMENT
This is a legal agreement between you ("Licensee") and Broadcom Corporation. ("BROADCOM"). BY OPENING THE SOFTWARE PACKAGE, CLICKING ON THE "ACCEPT" BUTTON OF ANY ELECTRONIC VERSION OF THIS END USER LICENSE AGREEMENT ("AGREEMENT") OR ACCESSING OR INSTALLING THE SOFTWARE, YOU ACKNOWLEDGE THAT YOU HAVE READ THE LICENSE AGREEMENT, UNDERSTAND IT AND AGREE TO BE BOUND BY ITS TERMS AND CONDITIONS. If you do not agree to the terms
I accept the terms in the license agreement
I do not accept the terms in the license agreement
InstallShield
< Back
Next >
Cancel

E

### 3 Click "I accept the terms in the license agreement" and click [Next].

Custom Set up window appears.


Broadcom Management Programs - InstallShield Wizard
Custom Setup
Select the program features you want installed.
Click on an icon in the list below to change how a feature is installed.
Control Suite
BASP
Feature Description
This feature will install the Broadcom Advanced Control Suite graphical user interface . This application contains a set of utilities supporting diagnostics, monitoring, and configuration for Broadcom network adapters.
This feature requires 2408KB on your hard drive.
InstallShield
Help
< Back
Next >
Cancel

### 4 Click [Next].

Proceed the installation by following the window instructions.

## For Windows Server 2003, Windows 2000 Server

**POINT**

- If the OS is installed using ServerStart, "BACS2" is already installed with the driver. If the OS is installed manually, BACS2 will not be installed.

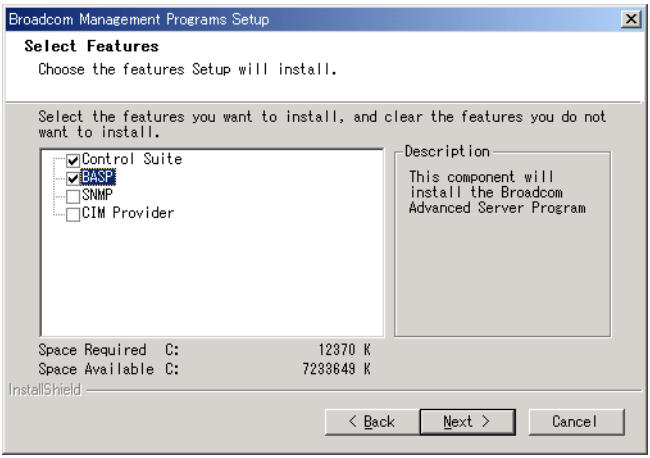
### 1 Start the following EXE file from the ServerStart Disc1 CD-ROM attached to the BX620 S4.

[CD-ROM drive]: \PROGRAMS\GENERAL\Broadcom\MgmtApps\setup.exe

The installer starts up.

### 2 Proceed the installation by following the window instructions.

When the window below appears during the installation procedure, check [BASP] and click [Next].


Broadcom Management Programs Setup
Select Features
Choose the features Setup will install.
Select the features you want to install, and clear the features you do not want to install.
Control Suite
BASP
SNMP
CIM Provider
Description
This component will install the Broadcom Advanced Server Program
Space Required C: 12370 K
Space Available C: 7233649 K
InstallShield
< Back
Next >
Cancel

E

# 5.3 Starting BACS2

To start BACS2, click "Control Panel" → "Broadcom Control Suite 2".
Click the tab that provides the information of interest or from which to perform a desired test, diagnostic, analysis, or set adapter properties.
To create a team, from the "Tools" menu, click [Create a Team], which starts the Teaming Wizard.

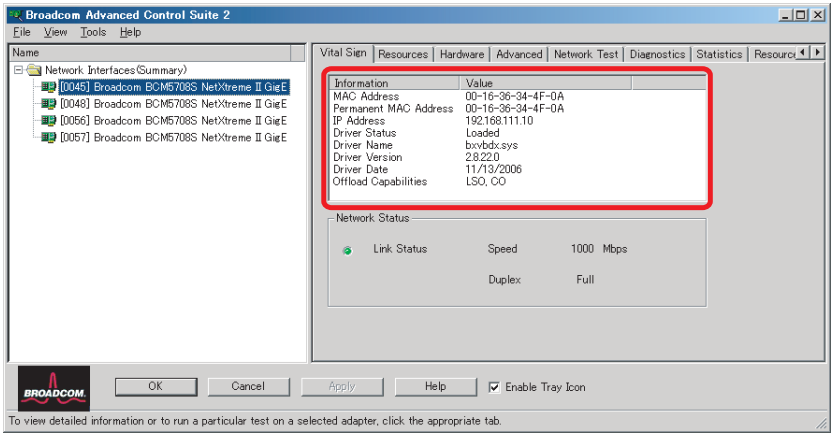
# 5.4 Setting of BACS2

## 5.4.1 Vital Sign

The "Vital Sign" tab shows useful information about 1Gbit/s Ethernet I/O Module, Onboard LAN, and other network adapters that are installed in your system. Such information includes the link status of the adapter and network connectivity. To view this information for each network adapter, click the name of the adapter listed in the "Name" pane.

**POINT**

- Information about Intel LAN card is less comprehensive than the information provided for this product.
- Some information may not be available for all network adapters.

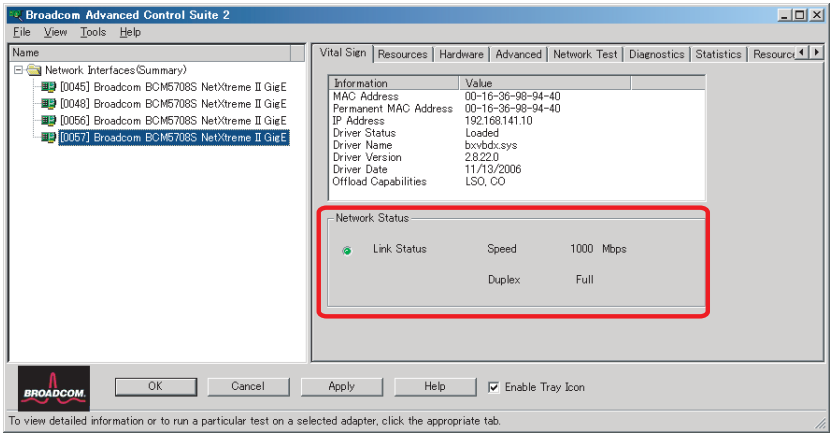



| Item | Description |
|---|---|
| MAC Address | This is the physical MAC address that is assigned to the adapter by the manufacturer. The physical address is never all 0s. |
| Permanent MAC Address | The unique hardware address assigned to the network adapter. |
| IP Address | The network address that is associated with the adapter. If the IP address is all 0s, this means that the associated driver has not been bound with Internet Protocol (IP). |

| Item | | Description |
|---|---|---|
| Driver Status | | The status of the adapter driver |
| | Loaded | Normal operating mode. The adapter driver has been loaded by Windows and is functioning. |
| | Not Loaded | The driver associated with the adapter has not been loaded by Windows. |
| | Information Not Available | The value is not obtainable from the driver that is associated with the adapter. |
| Driver Name/Version/Date | | The file name of the adapter driver. |
| LiveLink IP Address | | The network address of the LiveLink enabled adapter. |
| Offload Capabilities | | The offload capabilities supported by the adapter. |
| | LSO | Large Send Offload prevents an upper level protocol such as TCP from breaking a large data packet into a series of smaller packets with headers appended to them. |
| | CO | Checksum Offload allows the TCP/IP/UDP checksums for send and receive traffic to be calculated by the adapter hardware rather than by the host CPU. |
| BASP State | | Information about the status of the BASP application. This information is displayed only when there is a team (→"1.3.3 Teaming Function"(pg.109)). |

## Network Status

The following network status information is provided.

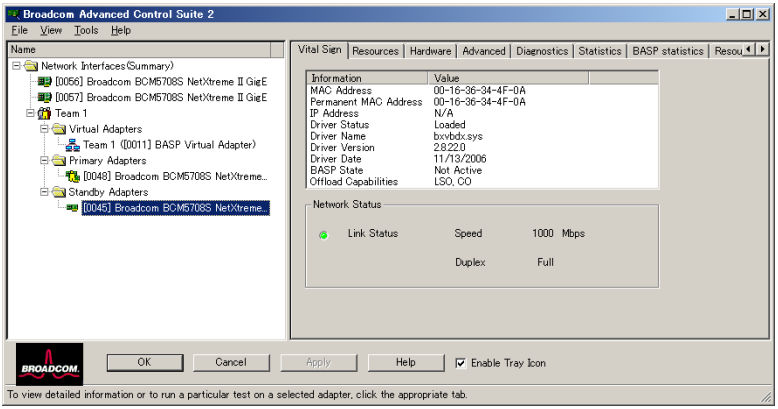



| Item | Description |
|---|---|
| Link Status | The indicator is green if a link is established. A red indicator means that a link is not established. |
| Speed | The link speed of the adapter |
| Duplex | The duplex mode in which the adapter is operating |

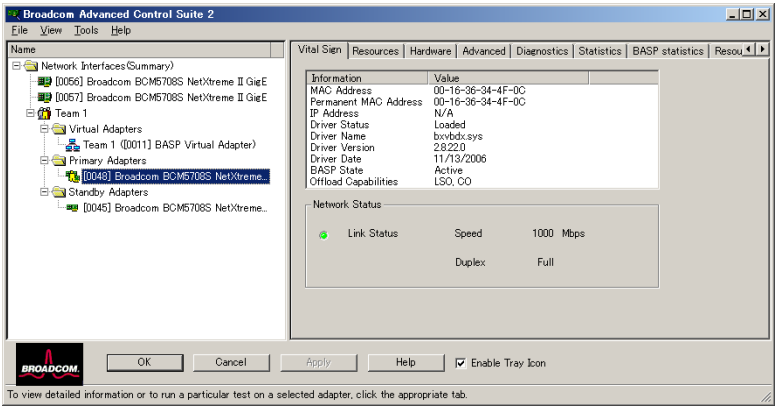
E

## Team Status

The team status is indicated by the appearance of the icons representing the team and the team members. If the adapter icon shows only the adapter, the adapter is connected to a network, but is not correctly participating in the team, which corresponds to a Not Active BASP state. This condition does not apply to an adapter that is a standby member of a team. The standby adapter may be working properly even though it is Not Active.




If the adapter icon shows a superimposed running yellow figure, the adapter is connected and participating in the team correctly, which corresponds to an Active BASP state.



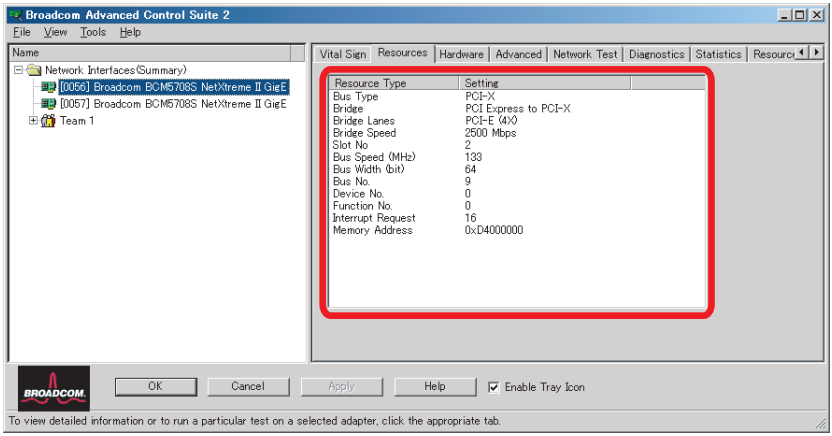

If the adapter icon shows a superimposed red letter X, the adapter is not connected to the network.

## 5.4.2 Resources

The following information can be checked on the "Resources" tab.

**POINT**

- Some information may not be available for all network adapters.



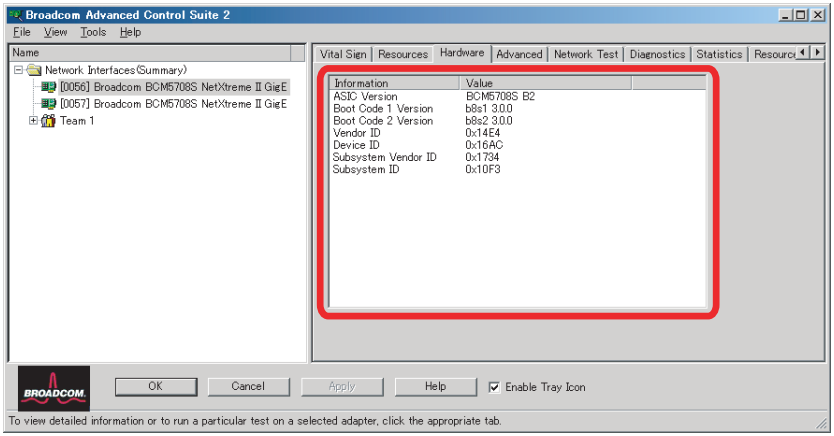

| Item | Description |
|---|---|
| Bus Type | The type of input/output (I/O) interconnect used by the adapter |
| Bridge | The bridge type, which is the PCI-E to PCI-X bridge. |
| Bridge Lanes | The number of PCI-E lanes connected to the bridge. |
| Bridge Speed | The clock speed on PCI-E bus. |
| Slot No | The slot number on the system board occupied by the adapter. |
| Bus Speed (MHz) | The bus clock signal frequency used by the adapter. |
| Bus Width (bit) | The number of bits that the bus can transfer at a single time to and from the adapter. |
| Bus No | Indicates the number of the bus in which the adapter is installed |
| Device No | The number assigned to the adapter by the operating system |
| Function No | The port number of the adapter. For a single-port adapter, the function number is 0. For a two-port adapter, the function number for the first port is 0, and the function number for the second port is 1. |
| Interrupt Request | The interrupt line number that is associated with the adapter. Valid numbers range from 2 to 25. |
| Memory Address | The memory mapped address that is assigned to the adapter. This value can never be 0. |

## 5.4.3 Hardware

The following information can be checked on the "Hardware" tab.

**POINT**

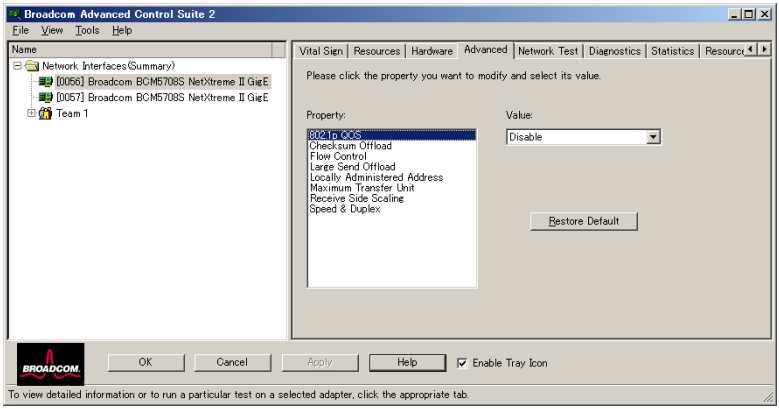
- Some information may not be available for all network adapters.




| Item | Description |
|---|---|
| ASIC Version | The chip version of the Broadcom adapter (this information is not available for adapters made by others). |
| Boot Code 1 Version | The version of boot code 1. |
| Boot Code 2 Version | The version of boot code 2. |
| Vendor ID | The vendor ID. |
| Device ID | The adapter ID. |
| Subsystem Vendor ID | The subsystem vendor ID. |
| Subsystem ID | The subsystem ID. |

## 5.4.4 Advanced

The following information can be checked on the "Advanced" tab.




The "Advanced" tab allows you to view and change the values of the available properties of the selected adapter. The potentially available properties and their respective settings are described below. To view the value of a property, click the name of the property in the "Property" list. The property value is displayed in the "Value" box. To change the value, click an item in the "Value" list or type a new value, as appropriate (selection options are different for different properties).

**POINT**

- You must have administrator privileges to change the values for a property.
- The list of available properties for your particular adapter may be different.
- Some properties may not be available for all network adapters.

| Item | Description |
|---|---|
| 802.1p QOS | The 802.1p QOS property enables quality of service, which is an Institute of Electrical and Electronics Engineering (IEEE) specification that treats different types of network traffic differently to ensure required levels or reliability and latency according to the type of traffic. This property is disabled by default. Unless the network infrastructure supports QoS, do not enable QoS. Otherwise, problems may occur. |

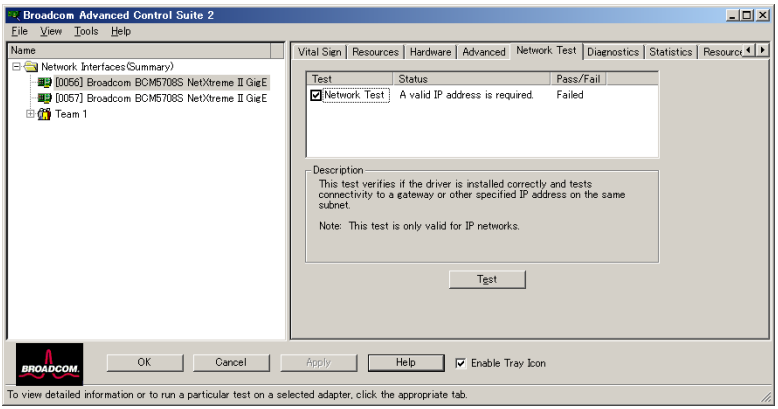
E

| Item | Description |
|---|---|
| Checksum Offload | Normally, the checksum function is computed by the protocol stack. When you select one of the Checksum Offload property values (other than None), the checksum can be computed by the network adapter.<br>• Rx TCP/IP Checksum<br>Enables receive TCP/IP/UDP checksum offload.<br>• Tx TCP/IP Checksum<br>Enables transmit TCP/IP/UDP checksum offload.<br>• Tx/Rx TCP/IP Checksum (default)<br>Enables transmit and receive TCP/IP/UDP checksum offload.<br>• None<br>Disables checksum offload. |
| Flow Control | The Flow Control property enables or disables the receipt or transmission of PAUSE frames. PAUSE frames enable the network adapter and a switch to control the transmit rate. The side that is receiving the PAUSE frame momentarily stops transmitting.<br>• Auto (default)<br>PAUSE frame receipt and transmission are optimized.<br>• Disable<br>PAUSE frame receipt and transmission are disabled.<br>• Rx PAUSE<br>PAUSE frame receipt is enabled.<br>• Rx/Tx PAUSE<br>PAUSE frame receipt and transmission are enabled.<br>• Tx PAUSE<br>PAUSE frame transmission is enabled. |
| Large Send Offload | Normally the TCP segmentation is done by the protocol stack. When you enable the Large Send Offload property, the TCP segmentation can be done by the network adapter.<br>• Disable<br>Disables Large Send Offload<br>• Enable. (default)<br>Enables Large Send Offload |

| Item | Description |
|---|---|
| Locally Administered Address | The Locally Administered Address is a user-defined MAC address that is used in place of the MAC address originally assigned to the network adapter. Every adapter in the network must have its own unique MAC address. This locally administered address consists of a 12-digit hexadecimal number.<br>• Value<br>Assigns a unique node address for the adapter<br>• Not Present (default)<br>Uses the factory-assigned node address on the adapter<br>The appropriate assigned ranges and exceptions for the locally administered address include the following:<br>• The range is 00:00:00:00:00:01 to FF:FF:FF:FF:FF:FD.<br>• Do not use a multicast address (least significant bit of the high byte = 1).<br>• Do not use all 0s or all F's. |
| Maximum Transfer Unit | The Maximum Transfer Unit property allows the network adapter to transmit and receive oversized Ethernet frames that are greater than 1514 bytes, but less than or equal to 9000 bytes in length. This property requires the presence of a switch that is able to process jumbo frames. Frame size is set at 1500 bytes by default. To increase the size of the received frames, increment the byte quantity in 500-byte increments. |
| Speed & Duplex | The Speed & Duplex property sets the connection speed and mode to that of the network. Note that Full-Duplex mode allows the adapter to transmit and receive network data simultaneously.<br>• 10 Mb Full<br>Sets the speed at 10 Mbit/s and the mode to Full-Duplex<br>• 10 Mb Half<br>Sets the speed at 10 Mbit/s and the mode to Half-Duplex<br>• 100 Mb Full<br>Sets the speed at 100 Mbit/s and the mode to Full-Duplex<br>• 100 Mb Half<br>Sets the speed at 100 Mbit/s and the mode to Half-Duplex<br>• Auto<br>Sets the speed and mode for optimum network connection802.1p QOS |

## 5.4.5 Network Test

On the "Network Test" tab, you can verify IP network connectivity. This test verifies if the driver is installed correctly and tests connectivity to a gateway or other specified IP address on the same subnet. Network Test uses TCP/IP. The network test sends ICMP packets to remote systems and waits for a response. If a gateway is configured, the test automatically sends packets to that system. If a gateway is not configured or if the gateway is unreachable, the test prompts you for a destination IP address.

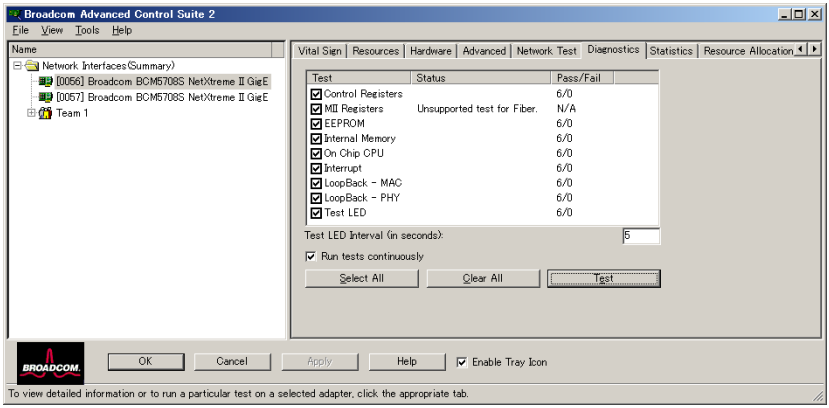



## 5.4.6 Diagnostics

On the "Diagnostics" tab, you can perform diagnostic tests on the physical components of a network adapter. The tests are continuously performed. The number of passes and fails in the "Pass/Fail" column increments each time the tests are performed. For example, if a test is performed four times and there are no fails, the value in the "Pass/Fail" column is 4/0. If there were 3 passes and 1 fail, however, the value in the "Pass/Fail" column is 3/1.

**POINT**

- You must have Windows administrator privileges to perform diagnostics.
- The network connection is temporarily lost when these tests are running.


Broadcom Advanced Control Suite 2
File View Tools Help
Name
Network Interfaces(Summary)
[0056] Broadcom BCM5708S NetXtreme II GigE
[0057] Broadcom BCM5708S NetXtreme II GigE
Team 1
Vital Sign Resources Hardware Advanced Network Test Diagnostics Statistics Resource Allocation
Test Status Pass/Fail
Control Registers 6/0
MII Registers Unsupported test for Fiber. N/A
EEPROM 6/0
Internal Memory 6/0
On Chip CPU 6/0
Interrupt 6/0
LoopBack - MAC 6/0
LoopBack - PHY 6/0
Test LED 6/0
Test LED Interval (in seconds): 5
Run tests continuously
Select All Clear All Test
OK Cancel Apply Help Enable Tray Icon
To view detailed information or to run a particular test on a selected adapter, click the appropriate tab.

| Item | Description |
|---|---|
| Control Registers | This test verifies the read and write capabilities of the network adapter registers by writing various values to the registers and verifying the results. The adapter driver uses these registers to perform network functions such as sending and receiving information. A test failure indicates that the adapter may not be working properly. |
| MII Registers | This test verifies the read and write capabilities of the registers of the physical layer (PHY). The physical layer is used to control the electrical signals on the wire and for configuring network speeds such as 1000 Mbit/s. |
| EEPROM | This test verifies the content of the electrically erasable programmable read-only memory (EEPROM) by reading a portion of the EEPROM and computing the checksum. The test fails if the computed checksum is different from the checksum stored in the EEPROM. An EEPROM image upgrade does not require a code change for this test. |
| Internal Memory | This test verifies that the internal memory of the adapter is functioning properly. The test writes patterned values to the memory and reads back the results. The test fails if an erroneous value is read back. The adapter cannot function if its internal memory is not functioning properly. |
| On-Chip CPU | This test verifies the operation of the internal CPUs in the adapter. |
| Interrupt | This test verifies that the Network Device Driver Interface Specification (NDIS) driver is able to receive interrupts from the adapter. |
| Loopback MAC and Loopback PHY | These tests verify that the NDIS driver is able to send packets to and receive packets from the adapter. |
| Test LED | This test causes all of the port LEDs to blink 5 times for the purpose of identifying the adapter. |

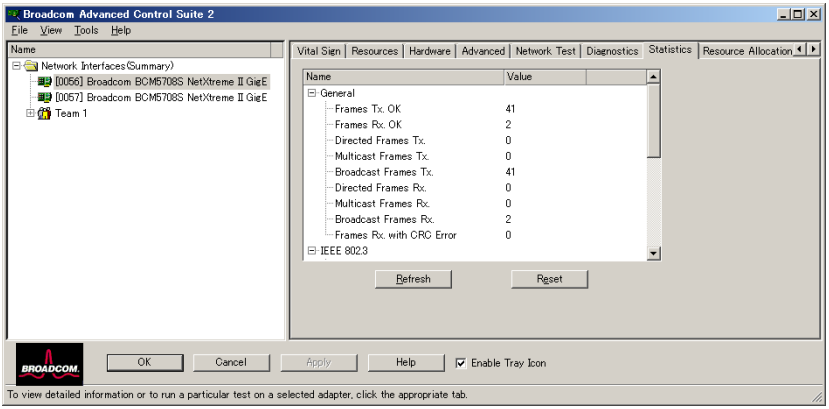
E

## 5.4.7 Statistics

On the "Statistics" tab, you can view traffic statistics for both Broadcom network adapters and network adapters made by others. Statistical information and coverage are more comprehensive for Broadcom adapters.

**POINT**

- Some statistics may not be available for all network adapters.




### General Statistics

| Item | Description |
|---|---|
| Frames Tx. OK | A count of the frames that were successfully transmitted. This counter is incremented when the transmit status is reported as Transmit OK. |
| Frames Rx. OK | A count of the frames that were successfully received. This does not include frames received with frame-too-long, frame check sequence (FCS), length, or alignment errors, or frames lost due to internal MAC sublayer errors. This counter is incremented when the receive status is reported as Receive OK. |
| Directed Frames Tx | A count of directed data frames that were successfully transmitted |
| Multicast Frames Tx. | A count of frames that were successfully transmitted (as indicated by the status value Transmit OK) to a group destination address other than a broadcast address. |
| Broadcast Frames Tx. | A count of frames that were successfully transmitted (as indicated by the transmit status Transmit OK) to the broadcast address. Frames transmitted to multicast addresses are not broadcast frames and therefore, are excluded. |
| Directed Frames Rx. | A count of directed data frames that were successfully received. |

| Item | Description |
|---|---|
| Multicast Frames Rx. | A count of frames that were successfully received and are directed to an active nonbroadcast group address. This does not include frames received with frame-too-long, FCS, length, or alignment errors, or frames lost because of internal MAC sublayer errors. This counter is incremented as indicated by the Receive OK status. |
| Broadcast Frames Rx. | A count of frames that were successfully received and are directed to a broadcast group address. This count does not include frames received with frame-too-long, FCS, length, or alignment errors, or frames lost because of internal MAC sublayer errors. This counter is incremented as indicated by the Receive OK status. |
| Frames Rx. with CRC Error | The number of frames received with CRC errors. |

## IEEE 802.3 Statistics

| Item | Description |
|---|---|
| Frames Rx. with Aligment Error | A count of the frames that were not an integral number of octets in length and do not pass the FCS check. This counter is incremented when the receive status is reported as Alignment Error. |
| Frames Tx. with One Collision | A count of the frames that were involved in a single collision and were subsequently transmitted successfully. This counter is incremented when the result of a transmission is reported as Transmit OK, and the attempt value is 2. |
| Frames Tx. with more than One Collision | A count of the frames that were involved in more than one collision and were subsequently transmitted successfully. This counter is incremented when the transmit status is reported as Transmit OK, and the value of the attempts variable is greater than 2 and less than or equal to the attempt limit. |
| Frames Tx. after Deferral | A count of the frames that were delayed being transmitted on the first attempt because the medium was busy. The frames involved in any collision are not counted. |

## Custom Statistics

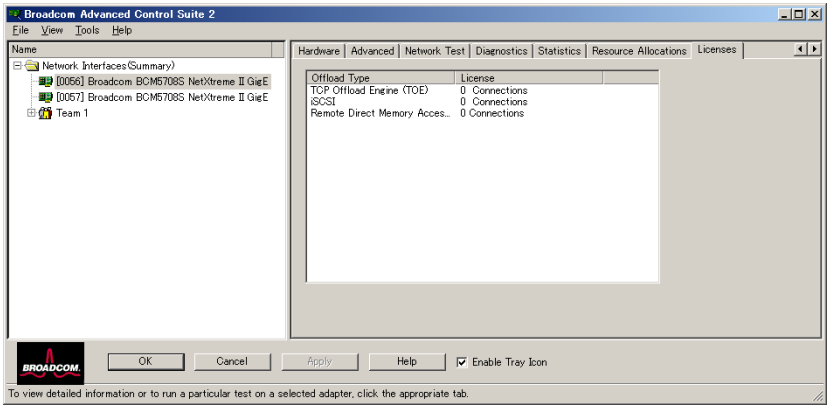
| Item | Description |
|---|---|
| Out of Recv. Buffer | The number of times the adapter ran out of Receive Buffer Descriptors. |
| Frames size less than 64-byte with bad FCS | The number of frames with a size less than 64 bytes with bad FCS. |
| MAC Rx w/ Pause Command and Length = 0 | MAC control frames with the pause command and a length equal to 0. |
| MAC Rx w/ Pause Command and Length greater than 0 | MAC control frames with the pause command and a length greater than 0. |
| MAC Rx w/ no Pause Command | MAC control frames with no pause command. |
| MAC Sent X-on | MAC Transmit with X-on was on. |
| MAC Sent X-off | MAC Transmit with X-on was off. |
| Large Send Offload Transmit Requests | The number of times the adapter was requested to transmit a packet performing TCP segmentation. |

## 5.4.8 Licenses

On the "Licenses" tab, you can view the number of connections available for TOE, iSCSI, and RDMA offload technologies. You can also upgrade your license for additional connections.

**POINT**

- The "Licenses" tab is only available for this product.
- Not all offload technologies are available with all adapters.



# 5.5 Configuring Teaming

The teaming function allows you to group any available network adapters together to function as a team. Teaming is a method of creating a virtual LAN (a group of multiple adapters that functions as a single adapter). The benefit of this approach is that it enables load balancing and failover. Teaming is done through the Broadcom Advanced Server Program (BASP) software. For a comprehensive description of the technology and implementation considerations of the teaming software, refer to →"4 Broadcom Gigabit Ethernet Teaming Services"(pg.119)

Teaming can be accomplished by either of the following methods:

- Using the Broadcom Teaming Wizard
  →"5.5.2 Creating and Modifying a Team Using the Teaming Wizard"(pg.177)
- Using Expert Mode
  →"5.5.3 Using Expert Mode"(pg.186)

**POINT**

- If you do not enable LiveLink™ when configuring teams, disabling Spanning Tree Protocol (STP) at the switch is recommended. This minimizes the downtime due to spanning tree loop determination when failing over. LiveLink mitigates such issues.
- BASP does not support Microsoft Network Load Balancing (NLB).
- The Large Send Offload (LSO), and Checksum Offload properties are enabled for a team only when all of the members support and are configured for the feature.
- You must have administrator privileges to create or modify a team.
- The load balance algorithm in a team environment in which members are connected at different speeds favors members connected with a Gigabit Ethernet link over members connected at lower speed links (100 Mbps or 10 Mbps) until a threshold is met. This is normal behavior.

For more details about Teaming, refer to "1.3.3 Teaming Function" (→pg.109).

**IMPORTANT**

- Link aggregation is not supported in the Blade Server.

## 5.5.1 Using the Broadcom Teaming Wizard

You can use the Broadcom Teaming Wizard to create a team, configure an existing team if a team has already been created, or create a VLAN.

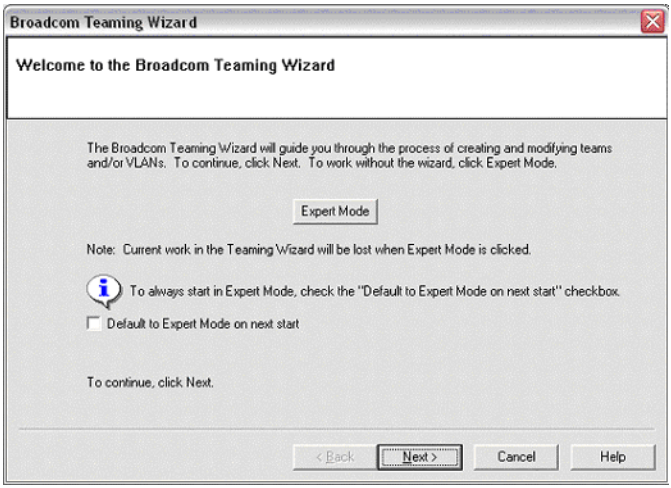
## 5.5.2 Creating and Modifying a Team Using the Teaming Wizard

### 1 On the BACS2 "Tools" menu, click "Create a Team".

**POINT**

- If you prefer to work without the wizard for now, click [Expert Mode] and then click [Next]. If you want to always use Expert Mode to create a team, select "Default to Expert Mode on next start" and then click [Next]. Refer to "5.5.3 Using Expert Mode" (→pg.186).

### 2 To continue using the wizard, click [Next].


Broadcom Teaming Wizard
Welcome to the Broadcom Teaming Wizard
The Broadcom Teaming Wizard will guide you through the process of creating and modifying teams and/or VLANs. To continue, click Next. To work without the wizard, click Expert Mode.
Expert Mode
Note: Current work in the Teaming Wizard will be lost when Expert Mode is clicked.
To always start in Expert Mode, check the "Default to Expert Mode on next start" checkbox.
Default to Expert Mode on next start
To continue, click Next.
< Back
Next >
Cancel
Help

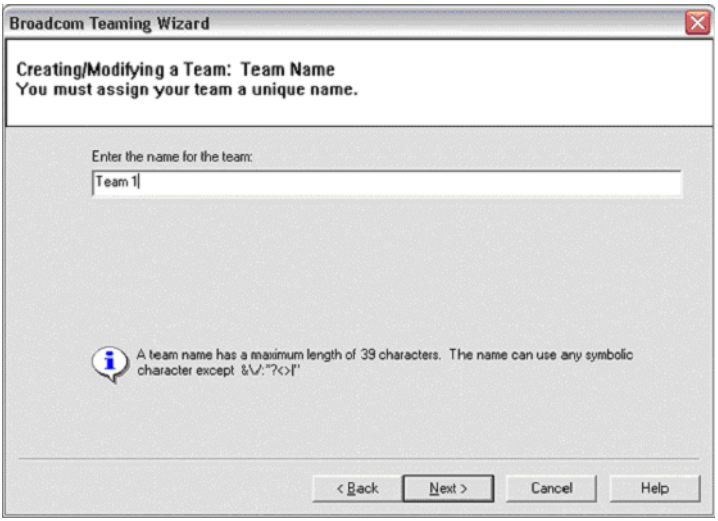
### 3 Type the team name and then click [Next].

- If you want to review or change any of your settings, click [Back].
- Click [Cancel] to discard your settings and exit the wizard.

**POINT**

- The team name cannot exceed 39 characters, cannot begin with spaces, and cannot contain any of the following characters: & \ / : * ? < > |

E


Broadcom Teaming Wizard
Creating/Modifying a Team: Team Name
You must assign your team a unique name.
Enter the name for the team:
Team 1
A team name has a maximum length of 39 characters. The name can use any symbolic character except &\/:*?<>|"
< Back
Next >
Cancel
Help

**4 Select the type of team you want to create and then click [Next].**

If the team type is an SLB type team, click [Next]. If the team type is not an SLB type team, then a dialog box appears.

Verify that the network switch connected to the team members is configured correctly for the team type, click [OK], and continue.

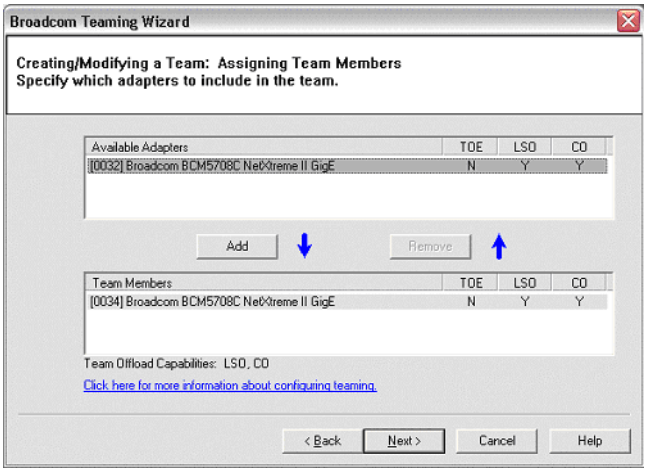
**5 From the "Available Adapters" list, click the adapter you want to add to the team and then click [Add].**

Remove team members from the "Team Members" list by clicking the adapter and then clicking [Remove]. Click [Next].

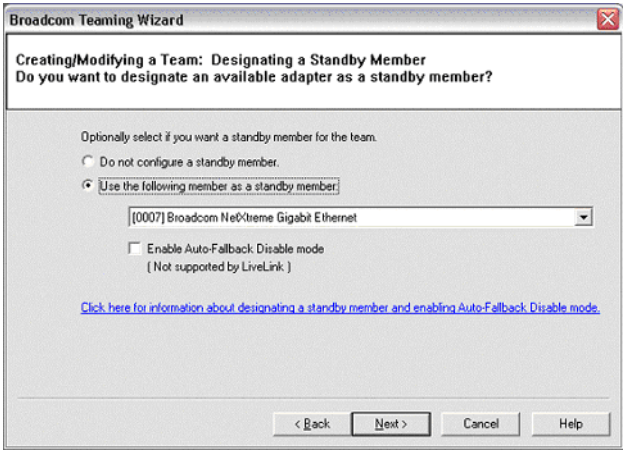
**POINT**

- There must be at least one network adapter assigned to the team.

The Large Send Offload (LSO) and Checksum Offload (CO) columns indicate if the LSO and/or the CO properties are supported (Y) or not supported (N) for the adapter. The LSO and CO properties are enabled for a team only when all of the members support and are configured for the feature. If this is the case, then the team offload capabilities appear on the bottom of the screen.




**6 If you want to designate one of the adapters as a standby member (optional), then click "Use the following member as a standby member".**


Broadcom Teaming Wizard
Creating/Modifying a Team: Designating a Standby Member
Do you want to designate an available adapter as a standby member?
Optionally select if you want a standby member for the team.
Do not configure a standby member.
Use the following member as a standby member:
[0007] Broadcom NetXtreme Gigabit Ethernet
Enable Auto-Fallback Disable mode
( Not supported by LiveLink )
Click here for information about designating a standby member and enabling Auto-Fallback Disable mode.
< Back
Next >
Cancel
Help

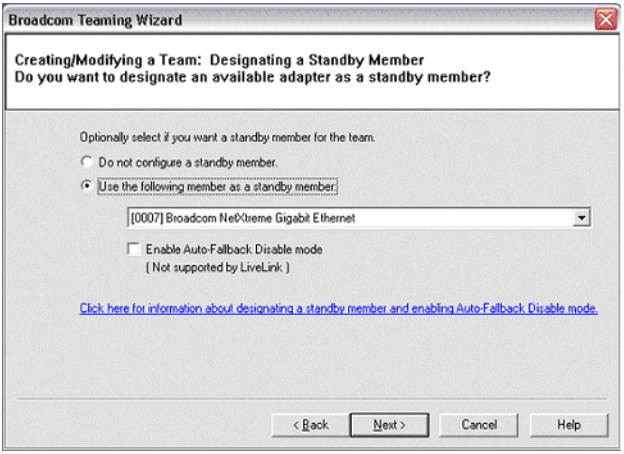
E

**7 Select the standby member from the list of adapters.**

The Auto-Fallback Disable mode feature allows the team to continue using the standby member rather than switching back to the primary member if the primary member comes back online.

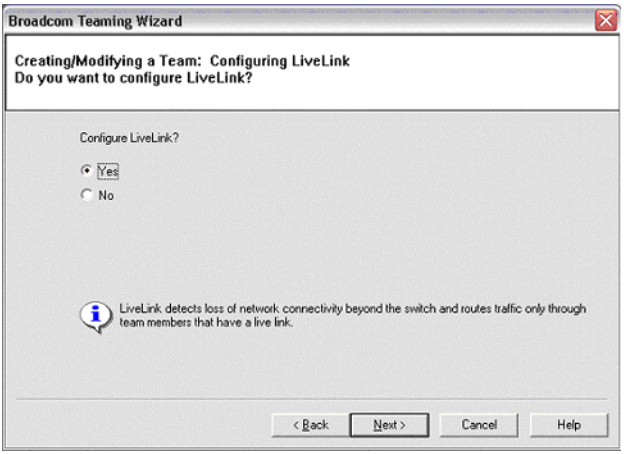
To enable this feature, click "Enable Auto-Fallback Disable mode" and then click [Next].

The Auto-Fallback Disable mode feature is enabled, LiveLink cannot be used.


Broadcom Teaming Wizard
Creating/Modifying a Team: Designating a Standby Member
Do you want to designate an available adapter as a standby member?
Optionally select if you want a standby member for the team.
Do not configure a standby member.
Use the following member as a standby member:
[0007] Broadcom NetXtreme Gigabit Ethernet
Enable Auto-Fallback Disable mode
( Not supported by LiveLink )
Click here for information about designating a standby member and enabling Auto-Fallback Disable mode.
< Back
Next >
Cancel
Help

**8 If you want to configure LiveLink, click [Yes] and then click [Next].**

If you do not want to configure LiveLink, click [No], and click [Next].

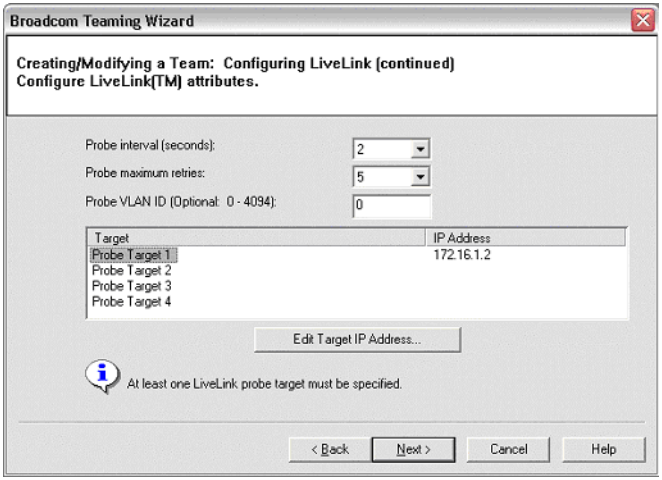

Broadcom Teaming Wizard
Creating/Modifying a Team: Configuring LiveLink
Do you want to configure LiveLink?
Configure LiveLink?
Yes
No
LiveLink detects loss of network connectivity beyond the switch and routes traffic only through team members that have a live link.
< Back
Next >
Cancel
Help

**9 Set the probe interval (the number of seconds between each retransmission of a link packet to the probe target) and the maximum number of probe retries (the number of consecutively missed responses from a probe target before a failover is triggered).**

**10 Click the probe target at the top of the list, click "Edit Target IP Address", type the target IP address in the "IP Address" box for one or all probe targets, and then click [OK]. Click [Next].**

**POINT**

- Only the first probe target is required. You can specify up to three additional probe targets to serve as backups by assigning IP addresses to the other probe targets.

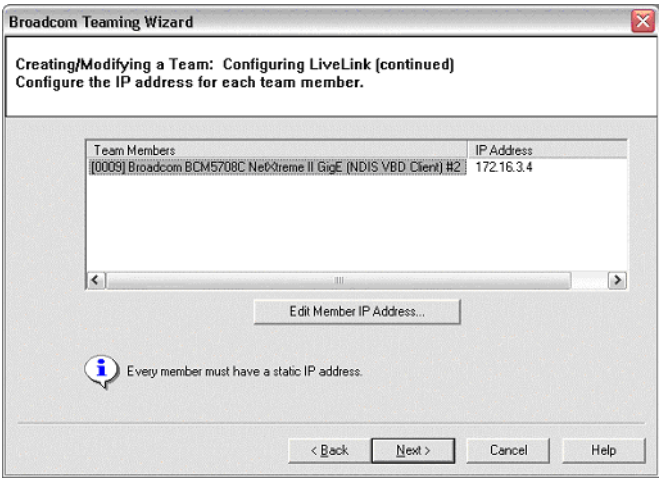



**11 Click a listed team member, click "Edit Member IP Address", and then type the member IP address in the IP Address box. Repeat for all listed team members and then click [OK]. Click [Next].**

**POINT**

- All of the member IP addresses must be in the same subnet as the subnet of the probe targets.

E


Broadcom Teaming Wizard
Creating/Modifying a Team: Configuring LiveLink (continued)
Configure the IP address for each team member.
Team Members
IP Address
[0009] Broadcom BCM5708C NetXtreme II GigE (NDIS VBD Client) #2
172.16.3.4
Edit Member IP Address...
Every member must have a static IP address.
< Back
Next >
Cancel
Help

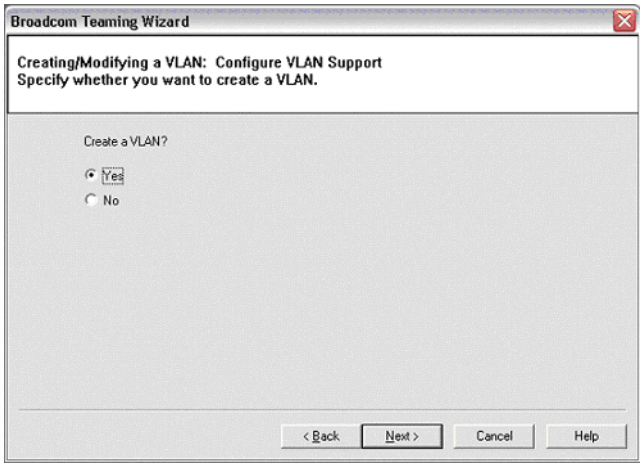
**12 If you want to create a VLAN on the team, click [Yes] and then click [Next].**

If you do not want to create a VLAN to the team, click [No], click [Next], and continue with the wizard from the "Finish" screen (refer to Step 17 of this procedure).

VLANs enable you to add multiple virtual adapters that are on different subnets. The benefit of this is that your system can have one network adapter that can belong to multiple subnets.

**POINT**

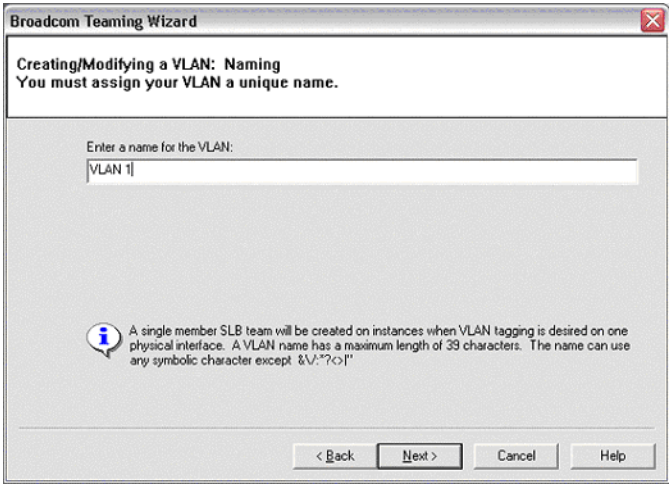
- VLANs can only be created when all team members are Broadcom adapters.




**13 Type the VLAN name and then click [Next].**

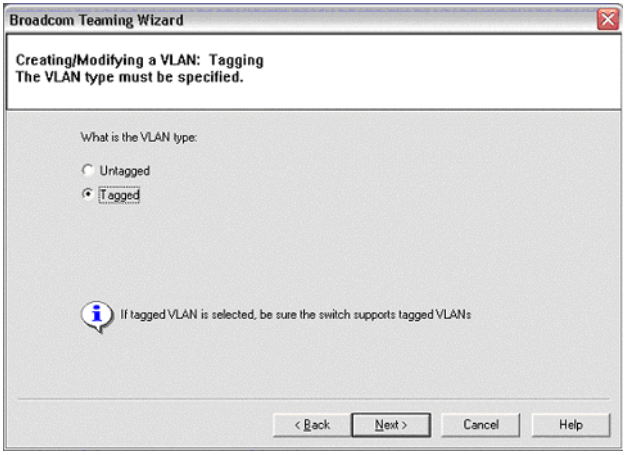
**POINT**

- The team name cannot exceed 39 characters, cannot begin with spaces, and cannot contain any of the following characters: & \ / : * ? < > |


Broadcom Teaming Wizard
Creating/Modifying a VLAN: Naming
You must assign your VLAN a unique name.
Enter a name for the VLAN:
VLAN 1
A single member SLB team will be created on instances when VLAN tagging is desired on one physical interface. A VLAN name has a maximum length of 39 characters. The name can use any symbolic character except &\/:*?<>|"
< Back
Next >
Cancel
Help

## 14 To tag the VLAN, click "Tagged" and then click [Next].

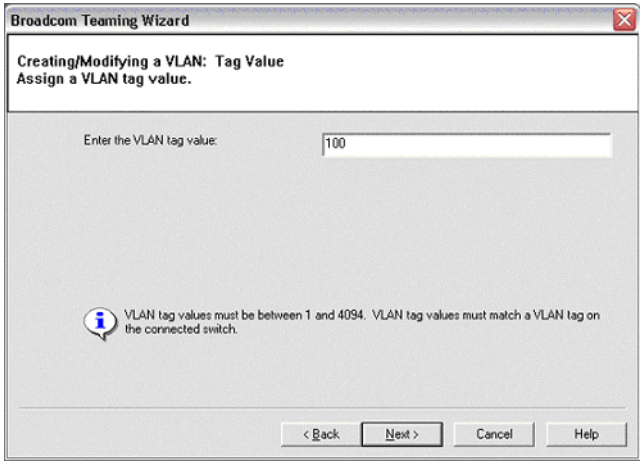
Otherwise, click "Untagged", click [Next], and continue with the wizard to add additional VLANs (refer to Step 16 of this procedure).




E

### 15 Type the VLAN tag value and then click [Next].

The value must be between 1 and 4094.

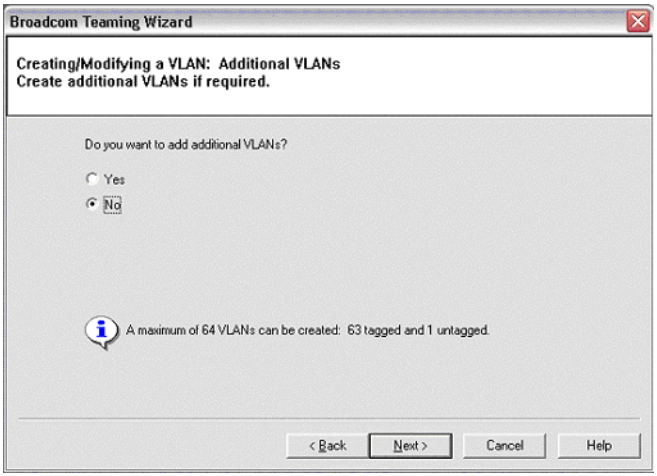

Broadcom Teaming Wizard
Creating/Modifying a VLAN: Tag Value
Assign a VLAN tag value.
Enter the VLAN tag value:
100
VLAN tag values must be between 1 and 4094. VLAN tag values must match a VLAN tag on the connected switch.
< Back
Next >
Cancel
Help

### 16 Click [Yes] to add another VLAN and then click [Next].

Repeat until you do not want to add any additional VLANs.

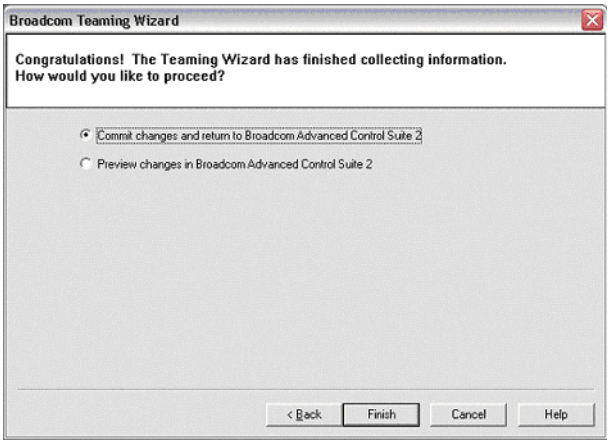
**POINT**

- You can define up to 64 VLANs per team (63 VLANs that are tagged and 1 VLAN that is not tagged). Adding several VLANS may slow down the reaction time of the Windows interface due to memory and processor time usage for each VLAN. The degree to which Windows performance may suffer depends on system configuration.


Broadcom Teaming Wizard
Creating/Modifying a VLAN: Additional VLANs
Create additional VLANs if required.
Do you want to add additional VLANs?
Yes
No
A maximum of 64 VLANs can be created: 63 tagged and 1 untagged.
< Back
Next >
Cancel
Help

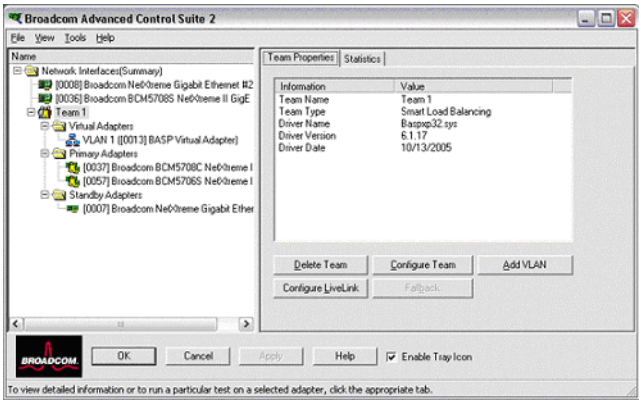
## 17 To apply and commit the changes to the team, click "Commit changes and return to Broadcom Advanced Control Suite 2" and then click [Finish].

To preview the changes to the team in BACS2, click "Preview changes in Broadcom Advanced Control Suite 2" and then click [Finish].
The wizard exits and BACS2 opens.


Broadcom Teaming Wizard
Congratulations! The Teaming Wizard has finished collecting information.
How would you like to proceed?
Commit changes and return to Broadcom Advanced Control Suite 2
Preview changes in Broadcom Advanced Control Suite 2
< Back
Finish
Cancel
Help

## 18 Click [Finish] to commit the changes.

Click [Cancel] to discard the changes.
Click the team to view the team's statistics from the "Statistics" tab and the team properties from the "Team Properties" tab.
Click the VLAN to view the properties of the VLAN from the "Vital Signs" tab.




E

## 5.5.3 Using Expert Mode

Use Expert Mode to create a team, modify a team, add a VLAN, and configure LiveLink for a Smart Load Balance and Failover team. To create a team using the wizard, refer to "5.5.2 Creating and Modifying a Team Using the Teaming Wizard" (→pg.177). To switch to the Teaming Wizard from the BACS2 "Tools" menu, click "Customize". Select the "Default Teaming Mode" tab and select "Wizard Mode".

### Creating a Team

**POINT**

- Enabling Dynamic Host Configuration Protocol (DHCP) is not recommended for members of an SLB type of team.

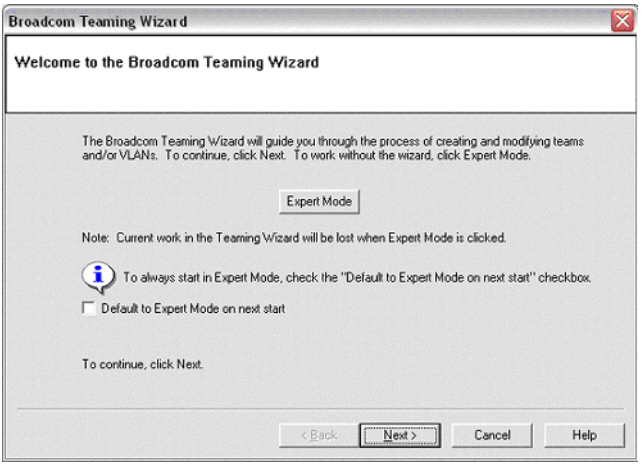
**1 Click the BACS2 "Tools" menu → "Create a Team".**

The wizard's Welcome screen appears.

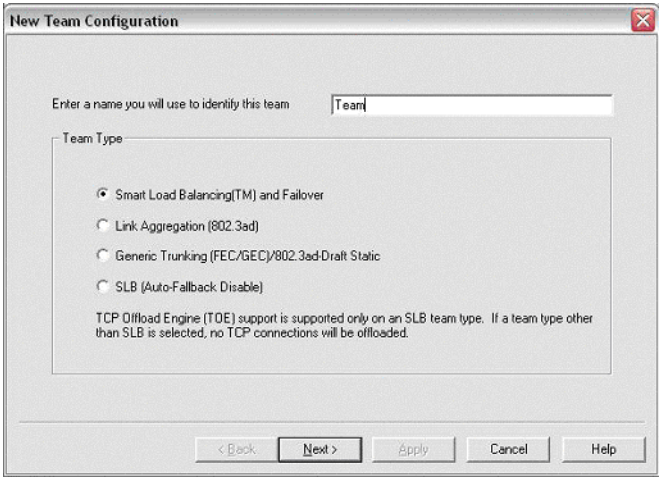
**2 To work without the wizard, click "Expert Mode".**

**POINT**

- If you want to always use Expert Mode to create a team, check "Default to Expert Mode on next start". Click [Next].


Broadcom Teaming Wizard
Welcome to the Broadcom Teaming Wizard
The Broadcom Teaming Wizard will guide you through the process of creating and modifying teams and/or VLANs. To continue, click Next. To work without the wizard, click Expert Mode.
Expert Mode
Note: Current work in the Teaming Wizard will be lost when Expert Mode is clicked.
To always start in Expert Mode, check the "Default to Expert Mode on next start" checkbox.
Default to Expert Mode on next start
To continue, click Next.
< Back
Next >
Cancel
Help

**3 Type a team name in the "Enter a name you will use to identify this team" box, and click the type of team, and then click [Next].**

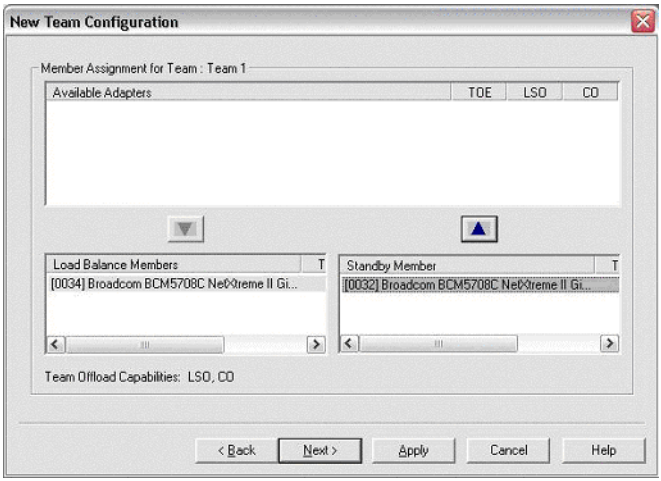

New Team Configuration
Enter a name you will use to identify this team
Team
Team Type
Smart Load Balancing(TM) and Failover
Link Aggregation (802.3ad)
Generic Trunking (FEC/GEC)/802.3ad-Draft Static
SLB (Auto-Fallback Disable)
TCP Offload Engine (TOE) support is supported only on an SLB team type. If a team type other than SLB is selected, no TCP connections will be offloaded.
< Back
Next >
Apply
Cancel
Help

**4 Assign any available adapter or adapters to the team by moving the adapter from the "Available Adapters" list to the "Load Balance Members" list.**

**5 Assign any other available adapter or adapters to the team by moving the adapter from the "Available Adapters" list to the "Standby Member" list.**

**POINT**

- There must be at least one network adapter assigned to the team.



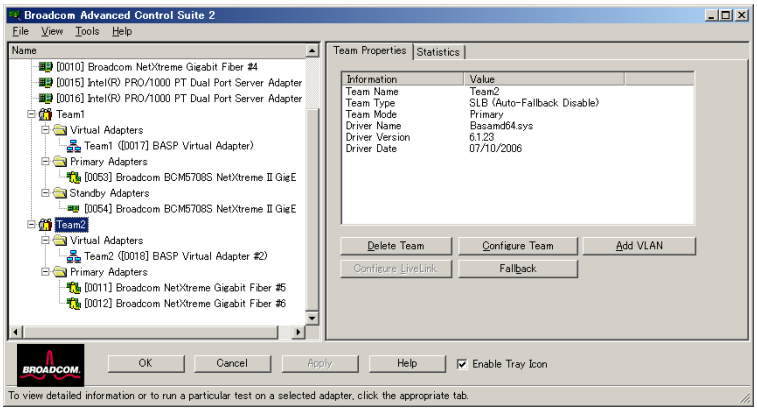

E

### 6 Click [Yes] when the message is displayed indicating that the network connection will be temporarily interrupted.

**POINT**

- The team name cannot exceed 39 characters, cannot begin with spaces, and cannot contain any of the following characters: & \ / : * ? < > |
- Team names must be unique. If you attempt to use a team name more than once, an error message is displayed indicating that the name already exists.
- The maximum number of team members is 8.
- When team configuration has been correctly performed, a virtual team adapter driver is created for each configured team.

- When you create Generic Trunking and Link Aggregation teams, you cannot designate a standby member.
  Standby members work only with Smart Load Balancing and Failover and SLB (Auto-Fallback Disable) types of teams.
- For an SLB (Auto-Fallback Disable) team, to restore traffic to the load balance members from the standby member, click the Fallback button on the "Team Properties" tab.




### 7 Configure the team IP address.

1. Click "Control Panel" → "Network Connections".
2. Right-click the name of the team to be configured, and then click "Properties".
3. On the "General" tab, click "Internet Protocol (TCP/IP)", and then click "Properties".
4. Configure the IP address and any other necessary TCP/IP configuration for the team, and then click [OK] when finished.

## Modifying a Team

After you have created a team, you can modify the team in the following ways:

- Change the type of team
- Change the members assigned to the team
- Add a VLAN
- Modify a VLAN (using Expert Mode)
- Remove a team or a VLAN (using Expert Mode)

The following shows how to modify a team.

1. **Click the BACS2 "Tools" menu → "Create a Team".**
   The wizard Welcome screen appears.
2. **Click [Next] to continue modifying a team using the wizard or click [Expert Mode] to work in Expert Mode.**
3. **Make the desired changes, and then click [OK].**
4. **Click [Apply].**
5. **Click [Yes] when the message is displayed indicating that the network connection will be temporarily interrupted.**

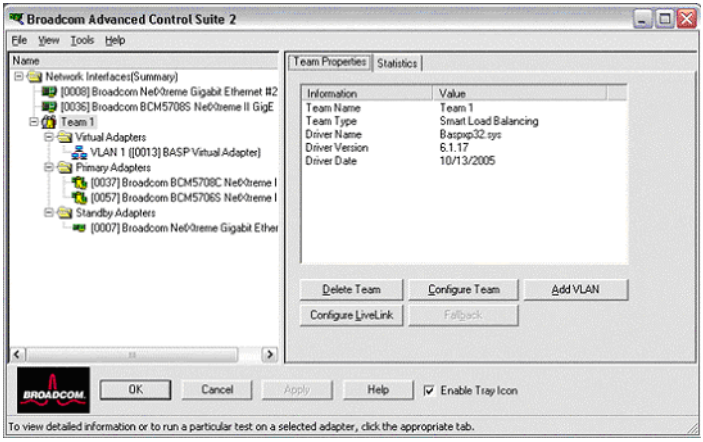
## Adding a VLAN

You also can add virtual LANs (VLANs) to a team. This enables you to add multiple virtual adapters that are on different subnets. The benefit of this is that your system can have one network adapter that can belong to multiple subnets. With a VLAN, you can couple the functionality of load balancing for the load balance members, and you can employ a failover adapter.

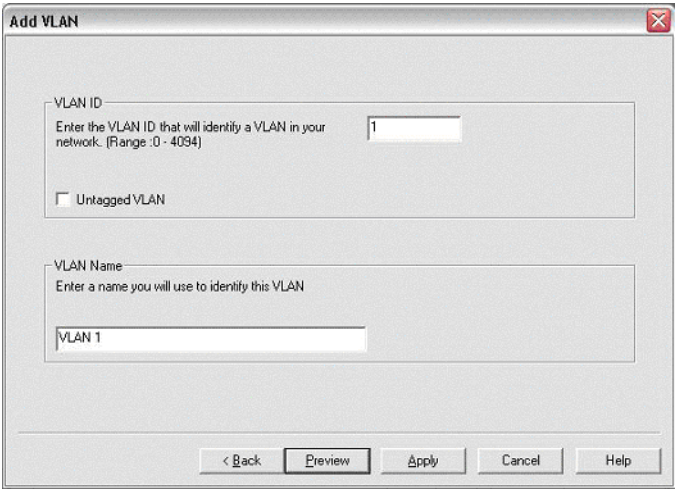
You can define up to 64 VLANs per team (63 VLANs that are tagged and 1 VLAN that is not tagged). VLANs can only be created when all teams members are Broadcom adapters. If you try to create a VLAN with a non-Broadcom adapter, an error message is displayed.

The following shows how to configure a team with a VLAN.

1. **Click the name of the team you want to configure.**
2. **From the "Team Properties" tab, click [Add VLAN].**



**3 Type the VLAN ID and VLAN name, and click [Apply].**




**POINT**

- If you type a VLAN name or ID and the name already exists, an error message is displayed.

**4 Click [Yes] when the message is displayed indicating that the network connection will be temporarily interrupted.**

**POINT**

- To maintain optimum adapter performance, your system should have 64 MB of system memory for each of the eight VLANs created per adapter.

## Viewing VLAN Properties and Running VLAN Tests

The following shows how to view VLAN properties and to run VLAN tests.

**1 Click the name of the VLAN adapter of interest.**

**2 Click the "Vital Sign" tab to view the properties of the VLAN adapter.**

**3 Click the "Network Test" tab to run a network test on the VLAN adapter.**

## Deleting a VLAN

To delete a VLAN, right-click the VLAN and select "Remove VLAN".

### 1 Click the "Tools" menu → "Configure a Team".

If there is more than one team, click the name of the team that has the VLAN you want to delete, and then click [OK].

### 2 Click [Remove VLAN].

### 3 Click [Apply].

Click [Yes] when the message is displayed indicating that the network connection will be temporarily interrupted.

**POINT**

- If you delete a team, any VLANs configured for that team are also deleted.

## Configuring LiveLink for a Smart Load Balancing and Failover Team

Read the following notes before you attempt to configure LiveLink.

**POINT**

- Before you begin configuring LiveLink™, review the description of LiveLink. Also verify that each probe target you plan to specify is available and working. If the IP address of the probe target changes for any reason, LiveLink must be reconfigured. If the MAC address of the probe target changes for any reason, you must restart the team. (→"4.8.10 Troubleshooting Teaming Problems"(pg.147).
- A probe target must be on the same subnet as the team, have a valid (not a broadcast, multicast, or unicast), statically-assigned IP address, and be highly available (always on).
- To ensure network connectivity to the probe target, ping the probe target from the team.
- You can specify up to four probe targets.
- The IP address assigned to either a probe target or team member cannot have a zero as the first or last octet.

E

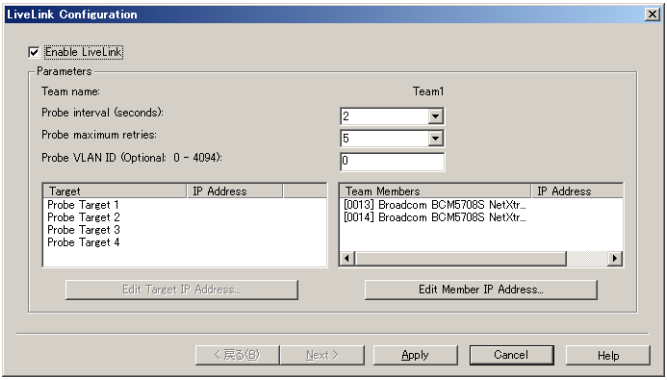
The following shows how to configure a LiveLink.

**1 Right-click the name of the Smart Load Balance and Failover (SLB) team, and then click "Configure LiveLink".**

**2 Check the "Enable LiveLink" box.**

It is recommended to accept the default values for "Probe interval" (the number of seconds between each retransmission of a link packet to the probe target) and "Probe maximum retries" (the number of consecutively missed responses from a probe target before a failover is triggered).

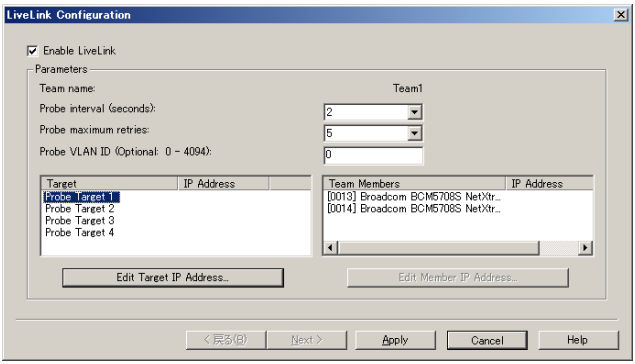
To specify different values, click the desired probe interval in the "Probe interval (seconds)" list and click the desired maximum number of probe retries in the "Probe maximum retries" list.




**3 Click the probe target at the top of the list, click "Edit Target IP Address", type the target IP address for one or all probe targets in the "IP Address" box, and then click [OK].**

**POINT**

- Only the first probe target is required. You can specify up to 3 additional probe targets to serve as backups by assigning IP addresses to the other probe targets.



4 **Click one of the listed team members, click "Edit Member IP Address", type the member IP address in the "IP Address" box, and then click [OK].**

POINT

- All of the member IP addresses must be in the same subnet as the subnet for the probe targets.

5 **Repeat step 4 for each of the other listed team members.**

6 **Click [Apply].**

## Configuring LiveLink in VLAN-tagged Environments

CAUTION

- For the teams with VLANs (on which LiveLink is enabled): to be able to communicate with the probe target, both the probe target and the team must be on an untagged VLAN (VLAN ID 0). Otherwise, the team loses connectivity.

1 **Ensure that the team has an untagged VLAN (VLAN ID 0).**

2 **Ensure there is network connectivity between the team and the probe target on the untagged VLAN.**

3 **Right-click the name of the SLB team with VLAN(s), and then click "Configure LiveLink".**

4 **Click the "Enable LiveLink" box.**

5 **Click the "desired probe interval" (the number of seconds between each retransmission of the link packet to the probe target) in the "Probe interval (seconds)" list.**

6 **Click the desired maximum number of probe retries in the "Probe maximum retries" list.**

7 **Click the probe target at the top of the list, click "Edit Target IP Address", type the target IP address in the "IP Address" box, and then click [OK].**

POINT

- It is not necessary to specify more than one probe target. If you do want to specify more than one, for each additional probe target (up to a total of 4), click the next probe target in the list, type the target IP address in the "IP Address" box, and then click [OK].

E

**8 Click one of the listed team members, click "Edit Member IP Address", type the member IP address in the "IP Address" box, and then click [OK].**

POINT

- All of the member IP addresses must be in the same subnet as the subnet for the probe targets.

**9 Repeat step 8 for each of the other listed team members.**

**10 Click [Apply].**

## Viewing the Team Properties and Statistics

The following shows how to view the team properties and statistics.

**1 Click the name of the newly created team.**

**2 Click the "Statistics" tab to view the team statistics.**

## Saving and Restoring a Configuration

The following shows how to save a configuration.

**1 Click the "File" menu → "Team Save As".**

**2 Type the path and file name of the new configuration file, and then click "Save".**

A .bcg extension is added. The configuration file is a text file that can be viewed by any text editor. The file contains information about both the adapter and the team configuration.

The following shows how to restore a configuration.

**1 Click the "File" menu → "Team Restore".**

**2 Click the name of the file to be restored, and then click [Open].**

POINT

- If necessary, go to the folder where the file is located.

**3 Click [Apply].**

**4 Click [Yes] when the message is displayed indicating that the network connection will be temporarily interrupted.**

If a configuration is already loaded, a message is displayed that asks if you want to save your current configuration.

Click [Yes] to save the current configuration. Otherwise, the configuration data that is currently loaded is lost.

# Appendix A Contact Information

- Australia:
  Fujitsu Australia Limited
  Tel: +61-2-9776-4555
  Fax: +61-2-9776-4556
  Address: 2 Julius Avenue (Cnr Delhi Road) North Ryde, Australia N.S.W. 2113
- China:
  Fujitsu (China) Holdings Co., Ltd.
  Tel: +86-21-5292-9889
  Fax: +86-21-5292-9566
  Address: 18F, Citic Square, 1168 West Nanjing Road Shanghai, China 200041
- Hong Kong:
  Fujitsu Hong Kong Limited
  Tel: +852-2827-5780
  Fax: +852-2827-4724
  Address: 10/F., Lincoln House, 979 King's Road Taikoo Place, Island East, Hong Kong
- Indonesia:
  PT. Fujitsu Systems Indonesia Offices Headquarters
  Tel: +62-21-570-9330 (Hunting)
  Fax: +62-21-573-5150
  Address: Wisma Kyoei Prince 10th Floor Jl. Jend. Sudirman Kav 3-4 Jakarta,
  Indonesia 10220
- Korea:
  Fujitsu Korea Ltd.
  Tel: +82-2-3787-6000
  Fax: +82-2-3787-6066
  Address: Susong Tower Building, 83-1 Susong-Dong Jongno-Gu, Seoul,
  Republic of Korea 110-140
- Malaysia:
  Fujitsu (Malaysia) Sdn. Bhd.
  Tel: +60-3-8318-3700
  Fax: +60-3-8318-8700
  Address: 1st Floor, No.3505 Jalan Technokrat 5 63000 Cyberjaya, Selangor Darul Ehsan Malaysia
- Philippines:
  Fujitsu Philippines, Inc.
  Tel: +63-2-812-4001
  Fax: +63-2-817-7576
  Address: 2nd Floor, United Life Building, A. Arnaiz Legaspi Village, Makati, Metro
  Manila Philippines

- Singapore:
  Fujitsu Asia Pte. Ltd.
  Tel: +65-6777-6577
  Fax: +65-6771-5502
  Address: 20, Science Park Road, #03-01 TeleTech Park, Singapore Science Park II, Singapore 117674
- Taiwan:
  Fujitsu Taiwan Limited
  Tel: +886-2-2311-2255
  Fax: +886-2-2311-2277
  Address: 19F, No.39, Section 1, Chung hwa Road Taipei, Taiwan
- Thailand:
  Fujitsu Systems Business (Thailand) Ltd.
  Tel: +66-2-500-1500
  Fax: +66-2-500-1555
  Address: 12th Floor, Olympia Thai Tower, 444 Rachadapisek Road Samsennok, Huaykwang, Bangkok, Thailand 10310
- Vietnam:
  Fujitsu Vietnam Limited
  Tel: +84-4-831-3895
  Fax: +84-4-831-3898
  Address: Unit 802-8th floor, Fortuna Tower Hanoi 6B Lang ha Street, Ba dinh District, Hanoi Socialist Republic of Vietnam
- United States:
  Fujitsu Computer Systems Corporation
  Tel: +1-800-831-3183
  Fax: +1-408-496-0575
  Address: 1250 East Arques Avenue, Sunnyvale, CA USA 94088-3470

For the latest information, refer to the Fujitsu PRIMERGY website (http://primergy.fujitsu.com).

**PRIMERGY**

LAN 拡張ボード（1Gbps）
（PG-LND201）
**取扱説明書**
1Gbit/s Ethernet I/O Module
（PG-LND201）
User's Guide

B7FY-2091-01-00

発 行 日　2007 年 5 月
発行責任　富士通株式会社

Issued on　May, 2007
Issued by　FUJITSU LIMITED

Printed in Japan

●本書の内容は、改善のため事前連絡なしに変更することがあります。
●本書に記載されたデータの使用に起因する、第三者の特許権およびその他の権利の侵害については、当社はその責を負いません。
●無断転載を禁じます。
●落丁、乱丁本は、お取り替えいたします。
• The contents of this manual may be revised without prior notice.
• Fujitsu assumes no liability for damages to third party copyrights or other rights arising from the use of any information in this manual.
• No part of this manual may be reproduced in any form without the prior written permission of Fujitsu.
• Any manual which has missing pages or which is incorrectly collated will be replaced.

Ⓟ

FUJITSU

古紙パルプ配合率100％再生紙を使用

このマニュアルはリサイクルに配慮して製本されています。
不要になった際は、回収・リサイクルに出してください。

*B7FY20910 1*